NEAR EAST UNIVERSITY

JOURNAL FOR ARTIFICIAL INTELLIGENCE AND INTERNET OF THINGS

Volume: 3 Issue:2

ISSN: 3062-1968

www.neu.edu.tr

JOURNAL OF ARTIFICIAL INTELLIGENCE AND INTERNET OF THINGS
International, Refereed Journal

November , 2024
Cilt-Volume 03/ Sayı-Issue 02

Foundation Year of the Journal
2022

Address and Contact
Yakın Doğu Üniversitesi İnovasyon ve Bilişim Teknolojileri Merkezi
International Research Center for AI and IoT
Yakın Doğu Bulvarı, PK: 99138Lefkoşa / KKTC Mersin 10 –TÜRKİYE
Tel:+90 (392) 223 64 64/+90 (392) 680 20 00Faks:+90 (392) 223 64 61
http://dergi.neu.edu.tr/ https://iot.neu.edu.tr/

Publication Contact

Prof. Dr. Fadi AL-TURJMAN

CONTENTS

CLOUD COMPUTING SERVICES FOR DISTRIBUTED MOBILE DEVICES

Ramiz Salama[1*], Chadi Altrjman[4], Fadi Al-Turjman[2, 3]

[1]Department of Computer Engineering, AI and Robotics Institute, Research Center for AI and IoT,
Near East University Nicosia, Mersin 10, Turkey
[2]Artificial Intelligence, Software, and Information Systems Engineering Departments, AI and Robotics Institute,
Near East University, Nicosia, Mersin10, Turkey
[3]Research Center for AI and IoT, Faculty of Engineering, University of Kyrenia, Kyrenia, Mersin10, Turkey
[4]Department of Chemical Engineering, Waterloo University, ON N2L 3G1, Canada
*Corresponding author Email: ramiz.salama@neu.edu.tr

Abstract

The advantages of cloud computing and mobile computing are combined in mobile cloud computing (MCC), which provides mobile devices with ubiquitous access to services, increased processing power, and storage capacity. In conventional cloud computing models, mobile devices use the internet to access centralized cloud resources. However, centralized systems have limitations in terms of responsiveness and efficiency as mobile apps become more complex and require real-time processing, faster performance, and lower latency. In response to these issues, a paradigm known as Distributed Mobile Cloud Computing (DMCC) has surfaced, in which cloud resources are dispersed over several sites, frequently nearer to the end users. This distributed architecture optimizes bandwidth utilization, lowers latency, and improves service availability by offloading processing activities from mobile devices via edge computing, fog computing, and cloudlets. DMCC makes it possible for resource-intensive applications to function well on mobile platforms, including augmented reality (AR), real-time data analytics, and sophisticated biometric authentication. Scalability, fault tolerance, and energy efficiency are promoted by the architecture's distribution of computational activities over a network of nearby and distant cloud resources. But it also brings with it additional difficulties including system complexity, effective resource allocation, and security threats. The basic ideas, design, and uses of distributed mobile cloud computing services are covered in this paper. It highlights the potential of DMCC to transform next-generation mobile applications and services by examining important technological issues and providing insights into new solutions.

Keywords: cloud computing, cloud computing services, and mobile cloud computing

1. Introduction

Numerous modeling techniques, including as software as a service, online storefronts, community networks, and cloud computing, have been developed as a result of advancements in networkbased computing. By offering remote access to material and apps, cloud computing enables thirdparty providers to offer services from any location, at any time, and in a variety of circumstances. A pay-per-use service, cloud computing offers software, memory, processing power, and storage as needed. Data centers, virtualization, and on-demand computing are its three main technologies. Resource consumption is optimized by task dispersion. Mobile Cloud

Computing, which centralizes computers and services for clients, has arisen with the popularity of smartphones. Distributed computing systems can be built using mobile devices, where each node is specified by a wireless communication architecture and a device [1–3]. As a result, Mobile Cloud Computing (MCC) has become popular, overcoming the limitations of mobile devices in terms of processing, storage, and networking. The main strategies for distributed cloud computing, important characteristics, and important mobile cloud computing technologies are covered in this review study.

2. Models for Cloud Deployment

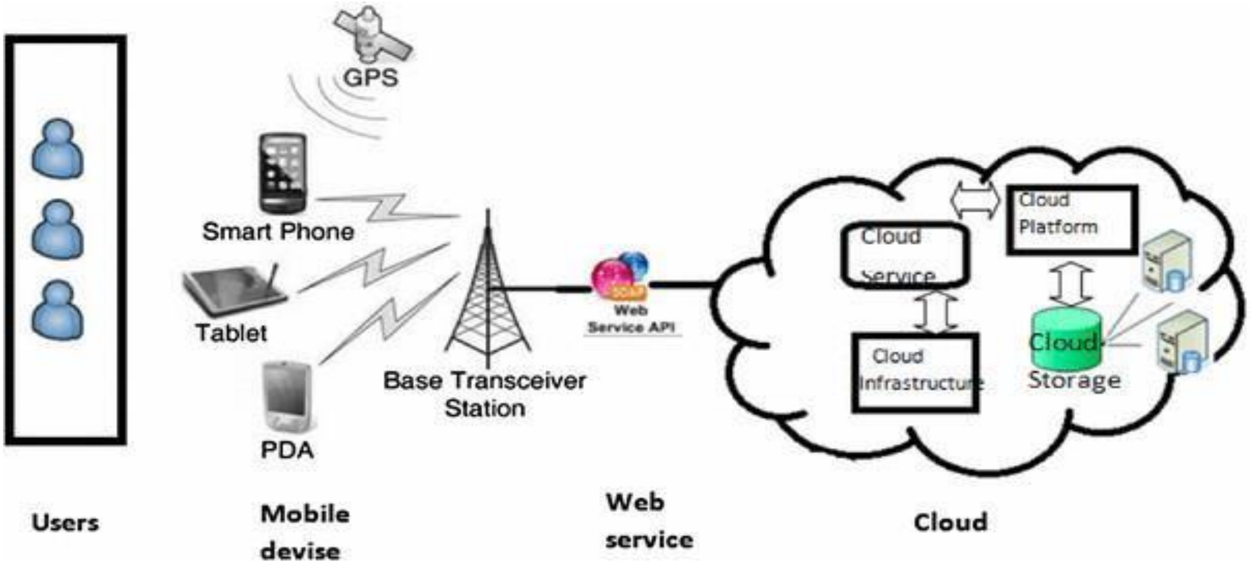


Figure1 Mobile Cloud Computing

Different application models based on service models can be implemented using cloud computing; Kumari and Singh (2021) have identified four main ones.

1) Private clouds provide improved data security, flexibility, scalability, and dependability and are customized for specific businesses or organizations.

2) Because of their widespread accessibility and suitability for storing non-sensitive data, public clouds—which are run by hosting companies—offer shared resource pools for service delivery, raising security concerns.

3) Deploying a community cloud entails sharing cloud infrastructure across several organizations in the community. This enables cooperative management by the community or a cloud service provider and permits remote access to stored files.

4) Hybrid cloud architecture combines public and private clouds to store data while preserving their unique identities for different deployment circumstances.

3. Models of Cloud Computing Services

With three tiers according to capacity and service provider model, cloud computing leverages computers, hardware, and networks to provide services. Customers may control components like operating systems and applications without having to worry about infrastructure upkeep thanks to Infrastructure as a Service (IaaS), which offers virtual computing resources like virtual machines. Using programming languages, resources, and tools that the cloud operator provides, PaaS is an internet-based platform for creating and sharing technologies and applications. By providing computer language libraries and tools for the development and deployment of applications, it makes software development easier. SaaS is a type of software delivery in which users obtain software over the cloud. Grid computing, parallel computing, and distributed computing are all included in cloud computing. For effective workload allocation, load balancing is essential. Cost reduction, geo-replication, redundancy, and dependability are all benefits of distributed cloud computing. It enhances data localization while reducing expenses and overheads associated with connectivity. Effective management of user needs requires efficient resource allocation [4–10]. Concerns about latency have led to the adoption of distributed clouds, particularly in data centerintensive scenarios such as cooperative document editing or gaming, where local clients include computers, robots, self-driving cars, and humans.

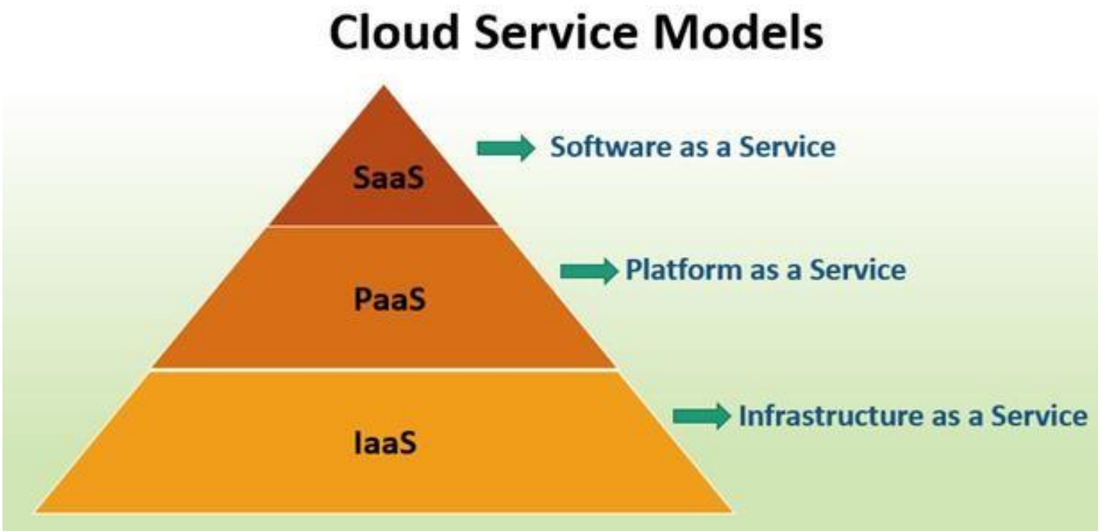


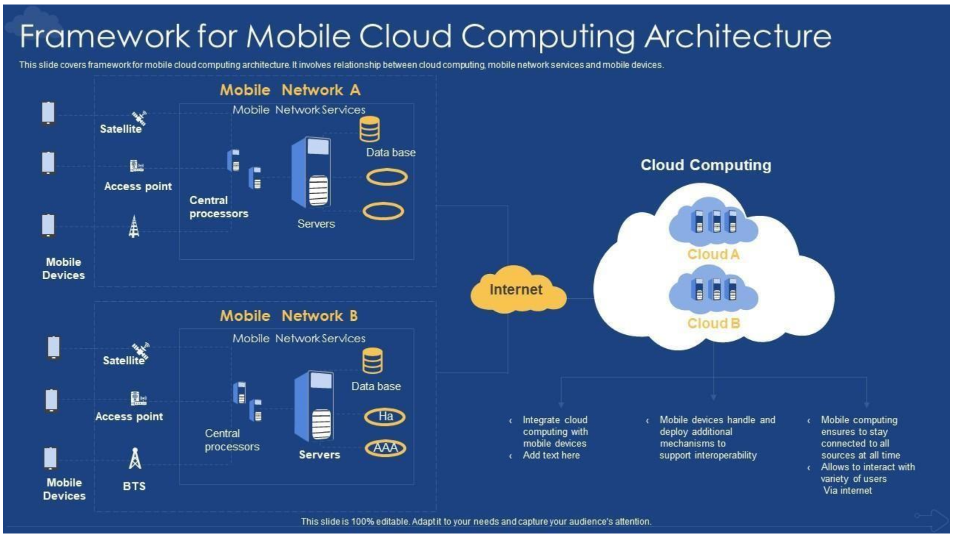
Figure 2. Cloud Service Models

4. Mobile Cloud Computing

Thanks to developments in networking, wireless technology, and mobile computing, the number of mobile users has increased dramatically, producing enormous amounts of data globally. The need for workplace mobility and the widespread use of sensors in mobile devices have led to the growth of mobile cloud computing, or MCC. In order to handle resource limitations in cellphones, MCC combines wireless networks, cloud computing, and mobile computing to manage and analyze data. Because wireless communication lines are vulnerable, mobile cloud computing (MCC) poses security risks. New privacy-conscious authentication techniques are required to counter this. Cloud computing and mobile devices must be integrated to optimize capabilities and overcome smartphone constraints. It is crucial to comprehend these traits in order to conduct additional study and development [11].

5. Architecture for Mobile Cloud Computing

Because of their many uses, mobile devices are becoming more and more commonplace in daily life. However, their designers must contend with resource limitations, such as limited CPU power and storage space. In order to get over these restrictions, Mobile Cloud computer (MCC) makes use of external computer resources. In the MCC architecture, tasks are carried out by mobile devices interacting with networking base stations. Because MCC architectural models include service-oriented architecture (SOA) layers, security considerations are essential. While the internet service layer links the mobile network to the cloud through fast connections, the mobile network layer links mobile users to cloud services through devices like smartphones and tablets [12]. A layer of cloud computing services provided by several service providers is known as the Cloud Services Provider Layer (MCC). It discusses smartphone processor power, storage capacity, battery life, and hardware constraints. MCC is crucial for contemporary mobile computing environments because it addresses hardware constraints and maximizes external computing resources.



Framework for Mobile Cloud Computing Architecture

This slide covers framework for mobile cloud computing architecture. It involves relationship between cloud computing, mobile network services and mobile devices.

- Integrate cloud computing with mobile devices
- Add text here

- Mobile devices handle and deploy additional mechanisms to support interoperability

- Mobile computing ensures to stay connected to all sources at all time
- Allows to interact with variety of users Via internet

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Figure 3. Mobile Cloud Computing Architecture

6. Mobile Cloud Computing's Advantages

Mobile cloud computing (MCC) is a valuable architecture that provides end users and enterprises with several advantages, such as simplicity of infrastructure construction and maintenance.

1. *Improving Battery Lifetime:* By shifting data processing and storage responsibilities to the cloud, especially for resource-intensive tasks that can rapidly drain the battery when carried out locally, MCC increases device battery life.
2. *Storage:* Cloud storage provides infinite capacity, removing the need to invest in server infrastructure and space issues, and lowering IT expenses related to hardware updates and maintenance for businesses.
3. *Improving Processing Power:* Applications that demand a lot of processing power, such as transcoding, gaming, and multimedia streaming, benefit from MCC's cloud-based processing capabilities.
4. *Disaster Recovery and Backup:* Unlike traditional physical storage solutions, cloud computing providers offer comprehensive backup and recovery services that streamline data backup and *restoration procedures and improve disaster recovery capabilities.*
5. *Scalability:* By allowing for scalability across web, cloud, and mobile devices, mobile apps can adjust to shifting user needs and meet different usage patterns.

6. *Reliability:* Cloud infrastructure outperforms individual devices in terms of security features like virus detection and authentication, guaranteeing the dependability and safety of cloud-based apps.

Beyond individual users, mobile cloud computing has a host of advantages for enterprises, such as improved performance, scalability, security, and dependability [13-30].

7. **Actual life uses for mobile cloud computing services that are dispersed.**

In order to increase speed, prolong battery life, and provide scalable, real-time services, distributed mobile cloud computing, or DMCC, combines mobile devices with cloud computing infrastructure. Distributed mobile cloud computing services have several practical uses, such as:

1. Smart Cities

- Traffic Management: By combining data from dispersed mobile devices, including smartphones, sensors, and cameras, DMCC assists in real-time traffic pattern analysis, improving traffic flow, and easing congestion.
- Environmental Monitoring: Temperature, noise levels, and air quality are measured by dispersed mobile sensors, which then process and analyze the data in the cloud. This enhances public health and encourages responsible environmental management.

2. Medical Care and Telemedicine

- Remote Monitoring: To provide ongoing health monitoring and prompt interventions, wearable technology and smartphone apps gather health data, including heart rate and blood sugar levels, which is then processed in the cloud.
- Medical Image Processing: Distributed clouds can process large medical pictures, such CT and MRI scans, giving clinician's remote access to improved diagnostic tools.

3. Augmented Reality (AR) and Virtual Reality (VR)

- Gaming and Entertainment: By shifting processing from mobile devices to cloud servers, DMCC enables resource-intensive AR/VR apps, providing immersive experiences while lowering latency and preserving responsiveness.
- Education and Training: To scale and provide low-latency experiences on mobile devices, AR/VR apps for remote learning and simulation-based training make use of distributed cloud computing.

4. Social Networks on the Go

- Content Sharing: Distributed mobile cloud computing eases the load on individual devices by processing and storing large volumes of images, videos, and other content in social media apps, allowing for rapid access to the media.
- Personalized Content Delivery: By analyzing user behavior and preferences, cloud services improve user experience by instantly delivering personalized content to mobile users.

5. IoT and Edge Computing

- Smart Homes: By shifting data processing to cloud infrastructure, distributed mobile clouds improve automation and efficiency by enabling real-time control of IoT devices (such as smart lights, thermostats, and security systems) through mobile apps.
- Industrial IoT (IIoT): DMCC analyzes data from dispersed sensors in manufacturing facilities to provide predictive maintenance and real-time monitoring, minimizing downtime and enhancing operational effectiveness.

6. MVNOs, or mobile virtual network operators

• Flexible Network Management: By using DMCC services to flexibly distribute network resources, MVNOs can provide scalable and reasonably priced mobile communication services in response to real-time demand, thereby enhancing user service quality.

7. Mobile Apps for Collaboration

• Crowdsourcing Platforms: Distributed mobile cloud computing is used by mobile apps that rely on user-generated content, like Waze (traffic data) or OpenStreetMap, to process and integrate data from multiple mobile devices and provide users with accurate and timely information. • Distributed Computing Projects: Apps such as SETI@home work with cloud services to do distributed computing tasks for research objectives by utilizing the idle processing power of mobile devices.

8. Mobile Cloud Gaming

• Game Streaming: By shifting processing and graphics rendering to robust cloud servers, DMCC allows cloud gaming platforms such as Google Stadia or Xbox Cloud Gaming to stream top-notch games to mobile devices while maintaining a fluid gameplay experience with low latency.

9. Retail and E-Commerce

- Mobile Payment Systems: By processing transactions in the cloud while upholding high security and low latency replies, DMCC guarantees the security and scalability of mobile payment apps (such as Apple Pay and Google Pay).
- Inventory Management: By processing and analyzing data in the cloud, retailers may optimize supply chain management and stock levels while managing inventory in real time across numerous stores using distributed mobile cloud computing.

These uses demonstrate how DMCC aids in resolving issues with scalability, throughput, and realtime data processing in a variety of sectors.

1. The potential applications of dispersed mobile cloud computing services.

A model known as Distributed Mobile Cloud Computing (DMCC) makes use of cloud computing resources dispersed among numerous mobile devices and edge servers. As it improves computing efficiency, latency, and resource usage by bridging the gap between cloud services and mobile devices, its potential is enormous. The following are some crucial areas for possible development:

1. Integration of 5G and Edge Computing

- Applications with Low Latency: By lowering latency and processing data closer to the edge, DMCC in conjunction with 5G networks makes real-time applications possible, such as driverless vehicles, virtual reality, and augmented reality.
- Decentralized AI: More individualized and contextually aware AI systems can be produced by training and running AI models on dispersed devices.

2. Smart Cities and IoT

• Real-Time Data Processing: DMCC will enable local data processing by Internet of Things (IoT) devices in smart cities, as well as the sharing of pertinent data with the cloud for more comprehensive analytics. Better trash management, energy saving, and traffic systems will result from this. • Improved Scalability: As the number of connected devices increases, distributed mobile clouds will enable the smart city infrastructure's quick scalability, enabling more effective resource management.

3. Efficiency in Energy Use

- Resource Optimization: By shifting computation-intensive jobs to dispersed clouds, mobile devices' energy usage can be optimized. The requirement for high-power computation on individual devices is decreased when workload is distributed evenly among devices, increasing overall system efficiency.

- Green Cloud Computing: By leveraging local computing resources, distributed mobile cloud computing can result in more energy-efficient systems by lowering data transit and, consequently, energy consumption in comparison to centralized cloud models.

4. Wearable technology and healthcare

- Telemedicine: By processing patient data from wearables and mobile sensors in real-time, mobile cloud computing may be essential to telemedicine, allowing for remote monitoring and quicker diagnosis.
- Distributed Health Data Management: By using edge computing to protect patient privacy, DMCC may enable distributed health records management, guaranteeing quicker access to patient data.

5. Security and Privacy of Data

• Decentralized Data Control: By integrating blockchain technology, DMCC can enhance data security and privacy by enabling decentralized data storage and access control systems, particularly in delicate industries like healthcare and finance. • Distributed Security Models: By lowering single points of failure, security procedures can be dispersed among nodes, increasing resistance to cyberattacks.

6. Virtual and Augmented Reality

- Real-Time Processing: By utilizing distributed mobile and edge resources, DMCC will make it possible for AR and VR apps to process data in real time. As a result, applications for leisure, education, and gaming will run more smoothly.
- Less Network Congestion: By shifting AR/VR data processing to the dispersed mobile cloud, centralized servers will be less taxed, allowing for quicker and more scalable content delivery.

7. Autonomous Systems

- Drones and Autonomous Vehicles: By processing data on edge nodes and neighboring devices, distributed mobile cloud services may allow autonomous systems, such as drones and self-driving automobiles, to make decisions more quickly.
- Collaborative Learning: Distributed learning models, in which drones and cars share real-time information, can help autonomous systems by eliminating the requirement for all processing to take place in central cloud data centers.

8. Gaming and Entertainment

- Cloud Gaming: With DMCC guaranteeing quicker reaction times, reduced latency, and improved user experiences, there will be a rise in demand for cloud gaming services. Workloads related to gaming could be transferred from mobile devices to dispersed cloud nodes.
- Streaming Services: By shifting processing duties to the edge, lowering latency, and delivering high-quality video, DMCC will maximize video streaming, particularly in areas with inadequate internet access.

9. Business and Enterprise Applications

• Mobile Enterprise Solutions: Companies will use DMCC more and more for remote and mobile workforce management, giving workers safe, effective access to cloud resources from any location. • Distributed Workflows: By distributing cloud services over several servers and mobile devices, enterprises can manage intricate workflows more effectively, increasing output and decreasing downtime.

10. Environmental Monitoring

Distributed Sensor Networks: Using IoT sensors dispersed throughout various places, mobile cloud computing may be utilized to monitor environmental variables in real time, such as water levels and air quality. Faster decision-making in disaster relief and climate change monitoring will be made possible by this [47].

11. Decentralized Finance (DeFi) and Blockchain

- Mobile Blockchain Nodes: By enabling mobile devices to function as nodes in a decentralized network, DMCC might facilitate blockchain applications by facilitating data sharing, smart contracts, and quicker and more secure financial transactions.
- Distributed Ledger Technology: By combining DMCC with distributed ledger technology, government operations, healthcare data, and financial institutions may become more transparent and secure.

12. Social Networks of the Next Generation

- Localized Content Sharing: By facilitating localized data processing and content sharing, improving privacy, and lessening the strain on centralized servers, DMCC can aid in the development of next-generation social networking platforms.
- Context-Aware Communication: By using DMCC, social networks can provide notifications and material in a way that is more contextually aware of the user's current surroundings and device capabilities [43][44].

Because of the increasing reliance on mobile devices, edge computing, the Internet of Things, and cloud infrastructure, distributed mobile cloud computing has a bright future with enormous potential across numerous industries. This paradigm, which offers improved performance, scalability, and sustainability, will influence technology in the future [45] [46].

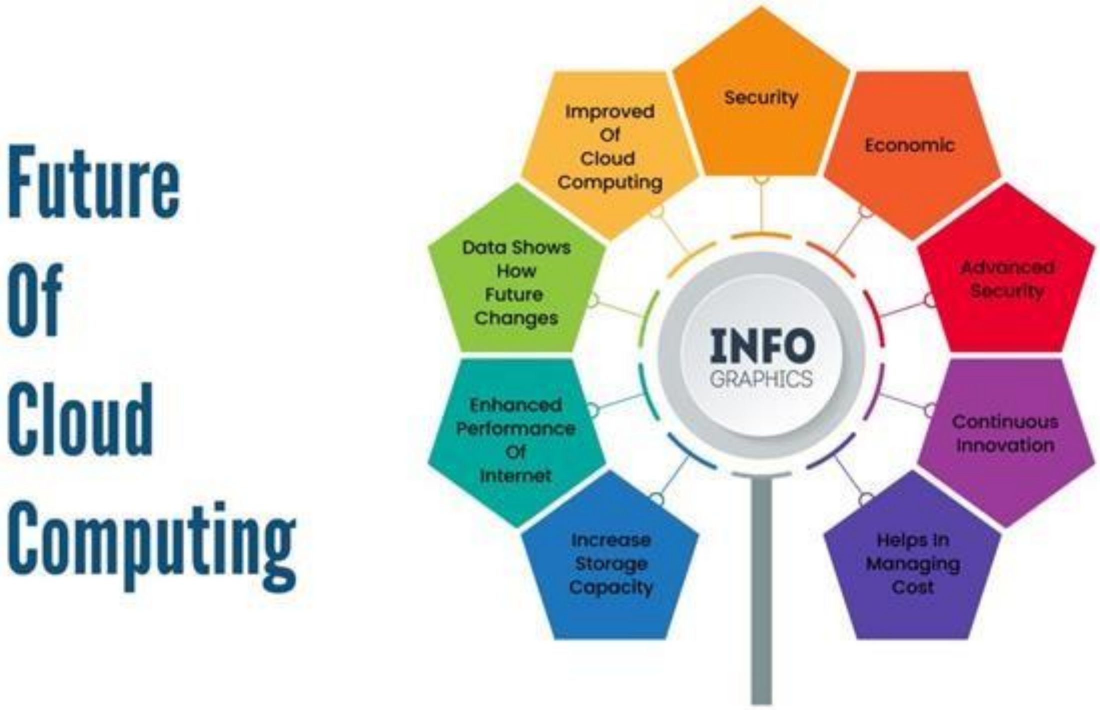

Future
Of
Cloud
Computing
INFO
GRAPHICS
Security
Economic
Advanced Security
Continuous Innovation
Helps In Managing Cost
Increase Storage Capacity
Enhanced Performance Of Internet
Data Shows How Future Changes
Improved Of Cloud Computing

Figure 4. Future of Cloud Computing

9. Conversation

Applications and data are integrated across regional borders by cloud computing, and distributed cloud computing makes collaborative workflows possible. No matter where they are, users can access computational resources using mobile cloud computing, facilitating sophisticated data processing and rich multimedia experiences. The combination of cloud and mobile technology spurs innovation across sectors and breaks down conventional barriers.

In cloud computing and mobile technology, load balancing is essential for maximizing efficiency and resource use. It optimizes power usage, increasing efficiency and prolonging the life of mobile devices. Modern computing paradigms are centered on the pursuit of scalability, with distributed and mobile cloud computing spearheading the movement toward adaptable computation and a more robust digital infrastructure [31-40].

Numerous advantages of distributed and mobile cloud computing include changing user interactions, spurring innovation in a variety of fields, and quickening the convergence of mobile and cloud technology [41][42].

Table (1): Summary of Distributed Cloud Computing.

Feature	(Z. A. S. A. et al Najat Z, 2019)	(Miguel Castanheira Sanches, n.d.)	(Salem, n.d.)
process a batch or a stream of data		✓	
support scalability		✓	
reduced latency times	✓	✓	
achieve high performance			
high resource utilization			
performing huge processing	✓		✓
utilizing power via cloud domain	✓	✓	
reduce a huge amount of processing power	✓	✓	✓

Table (2). Summary of Mobile Cloud Computing

Feature	(He et al., 2018)	(Z. A. S. A. et al Najat Z, 2019)	(Borcea et al., n.d.)	(Salem, n.d.)	(Mishra et al., n.d.)
solve a long-standing problem			✓		
identity-based signature scheme	✓				
less computation time	✓				
Fewer communication costs	✓				
parallel computations	✓	✓			
better performance	✓	✓			
power saving		✓			
Improve performance		✓		✓	
Huge Computation saving				✓	
Increasing Scalability					✓

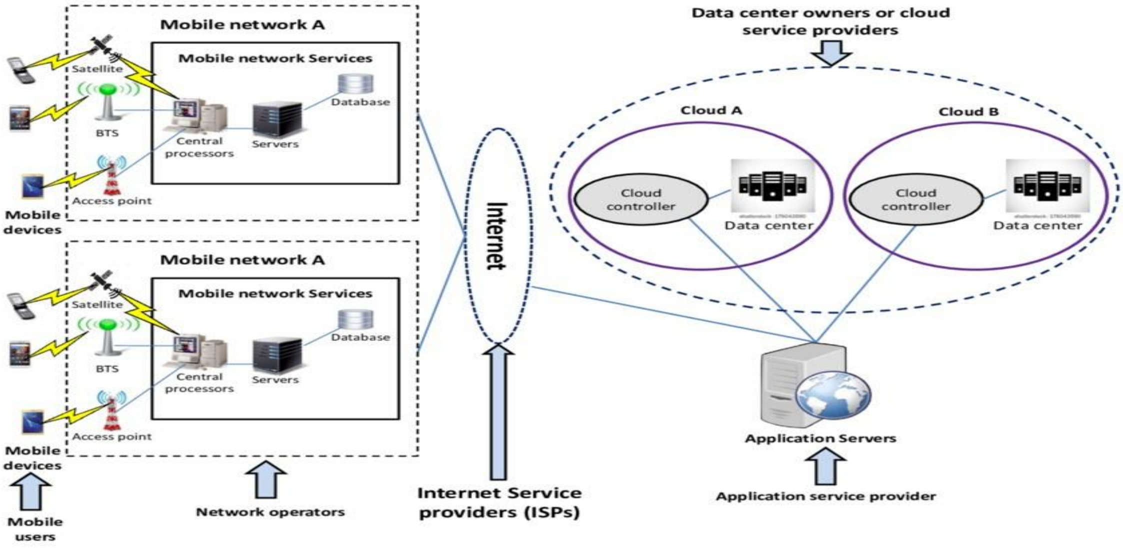


Figure 5. **A**n architecture for distributed mobile cloud computing

10. Conclusion

A careful examination of the details and comparison graphs in Section 6 makes it evident that mobile cloud computing and distributed cloud computing both have unique advantages and applications. Lowering latency times, offering high processing capacities, effectively using cloud electricity, and reducing major processing power requirements have been the main goals of previous distributed cloud computing research projects. Even though researchers have made great strides in enhancing data processing streams and facilitating scalability, there is still a gap in achieving optimal performance and resource consumption. However, mobile cloud computing, which prioritizes parallel processing and enhanced system efficiency, has emerged as a brilliant example of innovation. These advancements have solved long-standing problems such as identitybased signature systems, decreasing communication and calculation times, saving a significant amount of computation under high loads, and enhancing scalability. This study focuses on the area of mobile cloud computing, which the integration of cloud is computing into a mobile environment to enable users to access resources whenever they need them. Security protocols that are intended to prevent unauthorized access to sensitive data and information kept in the cloud are the main issues with mobile cloud computing. As we outline our future research plans, security concerns must be carefully taken into account while developing mobile cloud solutions. By addressing these security issues head-on, we can build a more robust and resilient mobile cloud ecosystem that meets users' evolving needs while upholding the highest standards of data privacy and security. In essence, despite offering distinct advantages and areas of focus, distributed cloud computing and mobile cloud computing both demonstrate the transformative potential of cloud technology in revolutionizing the digital world. As we navigate the complexities of a world that is becoming more interconnected, it is crucial to take advantage of the synergies between dispersed and mobile cloud computing. Customers will have unparalleled access to computing resources as a result, and cooperation and creativity will be encouraged. We can fully fulfill the potential of mobile cloud computing and usher in a new era of digital empowerment and excellence by utilizing thorough research and strategically placed investments in security and performance enhancement.

References

1. Asghari, A., & Sohrabi, M. K. (2024). Server placement in mobile cloud computing: A comprehensive survey for edge computing, fog computing and cloudlet. Computer Science Review, 51, 100616.
2. Afek, Y., Giladi, G., & Patt-Shamir, B. (2024). Distributed computing with the cloud. Distributed Computing, 37(1), 1-18.
3. Zangana, H. M., & Zeebaree, S. R. (2024). Distributed Systems for Artificial Intelligence in Cloud Computing: A Review of AI-Powered Applications and Services. International Journal of Informatics, Information System and Computer Engineering (INJIISCOM), 5(1), 11-30.
4. Bi, C., Li, J., Feng, Q., Lin, C. C., & Su, W. C. (2024). Optimal deployment of vehicular cloud computing systems with remote microclouds. Wireless Networks, 30(6), 5305-5317.
5. Mir, A. A. (2024). Optimizing Mobile Cloud Computing Architectures for Real-Time Big Data Analytics in Healthcare Applications: Enhancing Patient Outcomes through Scalable and Efficient Processing Models. Integrated Journal of Science and Technology, 1(7).
6. Kanwal, A., Amjad, T., & Ashraf, H. (2024). Framework for Agent-Based Multistage Application Partitioning Algorithm in Mobile Cloud Computing. SN Computer Science, 5(4), 330.
7. Khalaf, O. I., Anand, D., Abdulsahib, G. M., & Chandra, G. R. (2024). Original Research Article A coherent salp swarm optimization based deep reinforced neuralnet work algorithm for securing the mobile cloud systems. Journal of Autonomous Intelligence, 7(3).

8. Khalaf, O. I., Anand, D., Abdulsahib, G. M., & Chandra, G. R. (2024). Original Research Article A coherent salp swarm optimization based deep reinforced neuralnet work algorithm for securing the mobile cloud systems. Journal of Autonomous Intelligence, 7(3).
9. Dhanasekaran, S., Rajput, K., Yuvaraj, N., Aeri, M., Shukla, R. P., & Singh, S. K. (2024, May). Utilizing Cloud Computing for Distributed Training of Deep Learning Models. In 2024 Second International Conference on Data Science and Information System (ICDSIS) (pp. 1-6). IEEE.
10. Pramanik, P. K. D., Pal, S., & Choudhury, P. (2024). Mobile crowd computing: potential, architecture, requirements, challenges, and applications. The Journal of Supercomputing, 80(2), 2223-2318.
11. William, D., & Bommu, R. (2024). Harnessing AI and Machine Learning in Cloud Computing for Enhanced Healthcare IT Solutions. Unique Endeavor in Business & Social Sciences, 3(1), 70-84.
12. Raghav, Y. Y., & Kait, R. (2024). Edge computing empowering distributed computing at the edge. In Emerging Trends in Cloud Computing Analytics, Scalability, and Service Models (pp. 67-83). IGI Global.
13. Mahesar, A. R., Li, X., & Sajnani, D. K. (2024). Efficient microservices offloading for cost optimization in diverse MEC cloud networks. Journal of Big Data, 11(1), 123.
14. Anandappa, M., & Mudnal, M. K. (2024). Cloud computing and security issues in the cloud. Journal of Scientific Research and Technology, 59-66.
15. Rajagopalan, A., Swaminathan, D., Bajaj, M., Damaj, I., Rathore, R. S., Singh, A. R., ... & Prokop, L. (2024). Empowering power distribution: Unleashing the synergy of IoT and cloud computing for sustainable and efficient energy systems. Results in Engineering, 101949.
16. Asghari, A., & Sohrabi, M. K. (2024). Server placement in mobile cloud computing: A comprehensive survey for edge computing, fog computing and cloudlet. Computer Science Review, 51, 100616.
17. Zeebaree, I. (2024). The Distributed Machine Learning in Cloud Computing and Web Technology: A Review of Scalability and Efficiency. Journal of Information Technology and Informatics, 3(1).
18. Yadav, S. K., & Kumar, R. (2024). ASME-SKYR framework: A comprehensive task scheduling framework for mobile cloud computing. Wireless Networks, 30(3), 1221-1244.
19. Zangana, H. M., & Zeebaree, S. R. (2024). Distributed Systems for Artificial Intelligence in Cloud Computing: A Review of AI-Powered Applications and Services. International Journal of Informatics, Information System and Computer Engineering (INJIISCOM), 5(1), 11-30.
20. Dhinakaran, D., Selvaraj, D., Dharini, N., Raja, S. E., & Priya, C. (2024). Towards a novel privacy-preserving distributed multiparty data outsourcing scheme for cloud computing with quantum key distribution. arXiv preprint arXiv:2407.18923.
21. Hassan, M. U., Al-Awady, A. A., Ali, A., Iqbal, M. M., Akram, M., & Jamil, H. (2024). Smart Resource Allocation in Mobile Cloud Next-Generation Network (NGN) Orchestration with Context-Aware Data and Machine Learning for the Cost Optimization of Microservice Applications. Sensors, 24(3), 865.
22. Khalaf, O. I., Anand, D., Abdulsahib, G. M., & Chandra, G. R. (2024). Original Research Article A coherent salp swarm optimization based deep reinforced neuralnet work algorithm for securing the mobile cloud systems. Journal of Autonomous Intelligence, 7(3).
23. Mondal, R. (2024). Mobile Cloud Computing. In Emerging Trends in Cloud Computing Analytics, Scalability, and Service Models (pp. 170-185). IGI Global.
24. Alabdeli, H., Yamsani, N., Anitha, D., Chaithra, K. N., & Bindu, G. (2024, February). Intrusion Detection System in Mobile Cloud Computing Using Bat Optimization Algorithm-Support Vector Machine. In 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS) (pp. 1-4). IEEE.
25. Pramanik, P. K. D., Pal, S., & Choudhury, P. (2024). Mobile crowd computing: potential, architecture, requirements, challenges, and applications. The Journal of Supercomputing, 80(2), 2223-2318.
26. Vellela, S. S., & Balamanigandan, R. (2024). Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimedia Tools and Applications, 83(3), 7919-7938.
27. Fadhil, J., & Zeebaree, S. R. (2024). Blockchain for Distributed Systems Security in Cloud Computing: A Review of Applications and Challenges. Indonesian Journal of Computer Science, 13(2).
28. Fadhil, J., & Zeebaree, S. R. (2024). Blockchain for Distributed Systems Security in Cloud Computing: A Review of Applications and Challenges. Indonesian Journal of Computer Science, 13(2).
29. Anandappa, M., & Mudnal, M. K. (2024). Cloud computing and security issues in the cloud. Journal of Scientific Research and Technology, 59-66.
30. Taher, H., & Zeebaree, S. R. (2024). Harnessing the Power of Distributed Systems for Scalable Cloud Computing A Review of Advances and Challenges. Indonesian Journal of Computer Science, 13(2).
31. Khan, S., Jiangbin, Z., Irfan, M., Ullah, F., & Khan, S. (2024). An expert system for hybrid edge to cloud computational offloading in heterogeneous MEC–MCC environments. Journal of Network and Computer Applications, 225, 103867.
32. Verma, G. (2024). Blockchain-based privacy preservation framework for healthcare data in cloud environment. Journal of Experimental & Theoretical Artificial Intelligence, 36(1), 147-160.

33. Kumar, A., Boreda, D., & Vishwakarma, S. (2024, April). Redesigned Cloud Service Migration Techniques for Improved Portability. In 2024 IEEE 13th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 550-554). IEEE.
34. Soni, P. K., & Dhurwe, H. (2024). Challenges and Open Issues in Cloud Computing Services. In Advanced Computing Techniques for Optimization in Cloud (pp. 19-37). Chapman and Hall/CRC.
35. Murad, S. A., Azmi, Z. R. M., Muzahid, A. J. M., Sarker, M. M. H., Miah, M. S. U., Bhuiyan, M. K. B., ... & Bairagi, A. K. (2024). Priority based job scheduling technique that utilizes gaps to increase the efficiency of job distribution in cloud computing. Sustainable Computing: Informatics and Systems, 41, 100942.
36. Merseedi, K. J., & Zeebaree, S. R. (2024). The cloud architectures for distributed multi-cloud computing: a review of hybrid and federated cloud environment. Indonesian Journal of Computer Science, 13(2).
37. Jiang, Q., Xu, X., Bilal, M., Crowcroft, J., Liu, Q., Dou, W., & Jiang, J. (2024). Potential game based distributed IoV service offloading with graph attention networks in mobile edge computing. IEEE Transactions on Intelligent Transportation Systems.
38. Sinha, A., Banerjee, P., Roy, S., Rathore, N., Singh, N. P., Uddin, M., ... & Alsaqour, R. (2024). Improved Dynamic Johnson Sequencing Algorithm (DJS) in Cloud Computing Environment for Efficient Resource Scheduling for Distributed Overloading. Journal of Systems Science and Systems Engineering, 1-34.
39. Wang, Y., Yang, C., Lan, S., Zhu, L., & Zhang, Y. (2024). End-edge-cloud collaborative computing for deep learning: A comprehensive survey. IEEE Communications Surveys & Tutorials.
40. Kaur, S. (2024). Novel Encryption Technique for Cloud Computing Access Control. In Advancing Sustainable Science and Technology for a Resilient Future (pp. 323-326). CRC Press.
41. Larhgotra, A., Kumar, R., & Gupta, M. (2022, November). Traffic monitoring and management system for congestion comtrol using iot and ai. In *2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC)* (pp. 641-646). IEEE.
42. Kumar, R., Gupta, M., & Sapra, S. R. (2021, October). Speech to text community application using natural language processing. In *2021 5th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 1-6). IEEE.
43. Sharma, P., Kumar, R., Gupta, M., & Nayyar, A. (2024). A critical analysis of road network extraction using remote sensing images with deep learning. *Spatial Information Research*, 1-11.
44. Rao, H., Gupta, M., Agarwal, P., Bhatia, S., & Bhardwaj, R. (2024). Mental health issues assessment using tools during COVID-19 pandemic. *Innovations in Systems and Software Engineering*, *20*(3), 393-404.
45. Agarwal, S., & Chander Prabha, D. M. G. (2021). Chronic diseases prediction using machine learning–A review. *Annals of the Romanian Society for Cell Biology*, 3495-3511.
46. Gupta, M., Kumar, R., Chawla, S., Mishra, S., & Dhiman, S. (2021). Clustering based contact tracing analysis and prediction of SARS-CoV-2 infections. *EAI Endorsed Transactions on Scalable Information Systems*, *9*(35).
47. Kour, S., Kumar, R., & Gupta, M. (2021, October). Study on detection of breast cancer using Machine Learning.
    In *2021 International Conference in Advances in Power, Signal, and Information Technology (APSIT)* (pp. 1-9). IEEE.

6G NETWORKS POWERED BY BLOCKCHAIN TECHNOLOGY FOR INTELLIGENT MEDICALAPPLICATIONS

Ramiz Salama[1*], Sinem Alturjman[2, 3], Fadi Al-Turjman[2, 3]
[1]Department of Computer Engineering, AI and Robotics Institute, Research Center for AI and IoT,
Near East University Nicosia, Mersin 10, Turkey
[2]Artificial Intelligence, Software, and Information Systems Engineering Departments, AI and Robotics Institute,
Near East University, Nicosia, Mersin10, Turkey
[3]Research Center for AI and IoT, Faculty of Engineering, University of Kyrenia, Kyrenia, Mersin10, Turkey
*Corresponding author Email: ramiz.salama@neu.edu.tr

Abstract

The demand for intelligent, effective, and secure medical applications has increased due to the quick development of healthcare technologies. In order to provide complicated medical services, 6G networks promise ultra-high-speed communication, minimal latency, and huge interconnectedness. 6G networks can offer a strong and secure framework for intelligent medical applications when combined with blockchain technology, guaranteeing data accessibility, privacy, and integrity. By facilitating decentralized, transparent, and impenetrable medical data management, blockchain improves data security. By enabling smooth real-time data exchange between medical devices, patients, and healthcare professionals, this integration can provide more precise diagnosis, effective treatment, and individualized healthcare solutions. With a focus on important use cases including telemedicine, remote patient monitoring, and AI-based diagnostics, this paper examines how blockchain-powered 6G networks have the potential to transform healthcare by offering intelligent, scalable, and secure medical services..

Keywords: 6G networks, blockchain technology, and smart healthcare

1. Introduction

This article examines how blockchain technology can be incorporated into healthcare systems, emphasizing how it can be enhanced when paired with 6G networks.

Blockchain is a secure, decentralized ledger technology that improves healthcare efficiency, privacy, and data integrity. It functions over a network of computers, or nodes, in which a cryptographic hash connects each transaction. A highly safe and transparent system is produced as a result of this decentralization, which does away with the need for a central authority to supervise transactions. Because of its revolutionary potential, blockchain makes it possible to securely store and exchange patient records, treatment histories, and other private medical data, which lowers expenses and boosts productivity [1–3]. The influence of the technology is further increased by smart contracts, which automatically activate predetermined conditions.

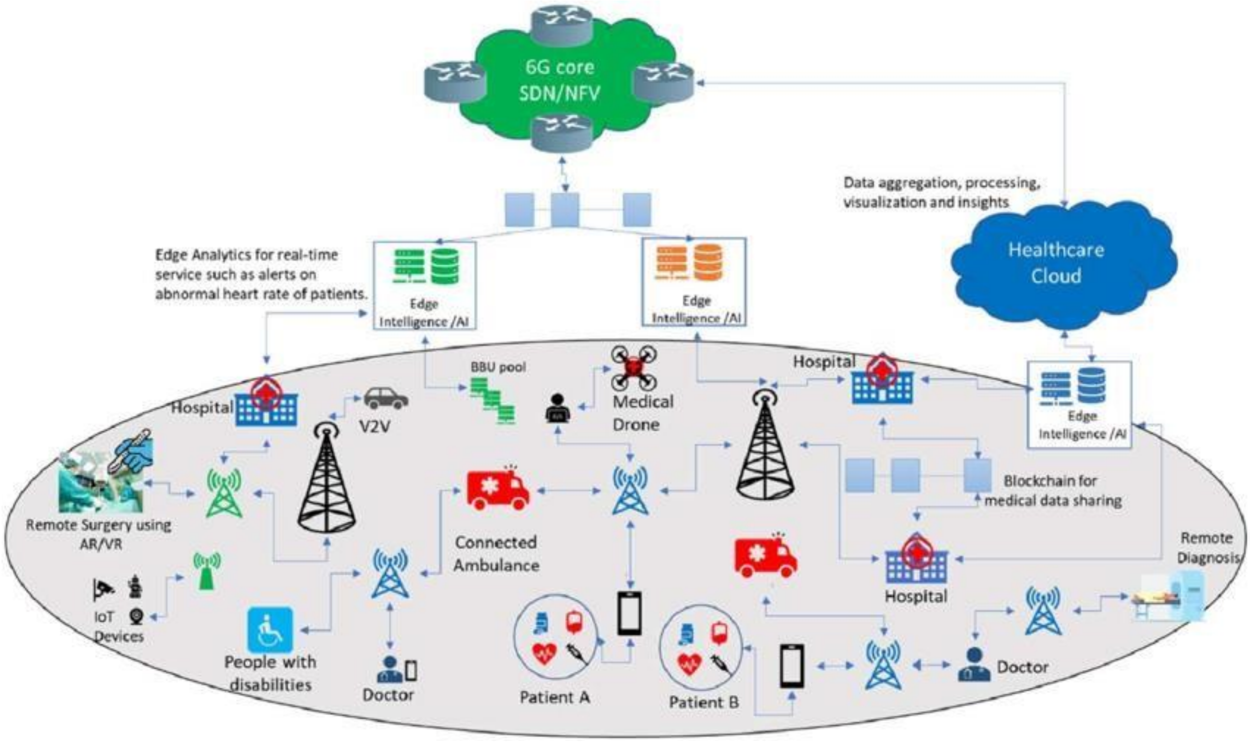


Figure 1. 6G Enabled-IoT for future Smart healthcare.

1.1. Using Blockchain Technology in Medical Practice

The essay explores the ways in which blockchain technology might be used in healthcare to address persistent issues including data security, transparency, and interoperability. The investigation of its possibilities prepares the ground for the discussion of 6G networks that follows. Blockchain integration in healthcare signifies a revolutionary change in the way the sector handles, preserves, and disseminates private medical data. The various facets of how blockchain smoothly becomes an essential part of the healthcare ecosystem are explored in this section. The safe and compatible transfer of patient data across different organizations, including clinics, hospitals, and insurance companies, is one of the biggest problems in the healthcare industry. Blockchain solves this by providing a distributed, decentralized ledger that guarantees the accuracy and unchangeability of medical records. There is only one source of truth for all parties involved because every network participant has an identical copy of the ledger [4,5].

1.2. Strengthening Security via Dispersion

The decentralization of blockchain ensures safe data distribution throughout the network by removing a central point of vulnerability. In addition to improving security, this gives people more authority over their health information, protecting privacy and adhering to HIPAA rules.

1.3. Streamlined Interaction

Blockchain overcomes interoperability issues by offering a standardized, secure framework for data sharing, enabling automated transactions between healthcare systems.

1.4. Audible and Clear

By safely recording transactions, lowering errors, fraud, and illegal access, and encouraging a more dependable and accountable environment, blockchain improves the trust in the healthcare system.

1.5 Supply chain management and medication traceability

Blockchain improves pharmaceutical and medical device traceability across the supply chain, guaranteeing authenticity and enabling quick action in the event of an emergency or recall.

1.6 Empowerment of Research and Development

Blockchain technology in healthcare provides safe, private data exchange, speeding up medical research and maybe resulting in treatment breakthroughs. It has an impact on supply chain logistics and creates a cooperative setting for research and development, opening the door to an ecosystem that is safer, more effective, and more patient-friendly.

1.7 6G Communications' Significance

By providing revolutionary features that work in tandem with blockchain, 6G networks expand the potential of blockchain in the healthcare space and open the door for intelligent healthcare applications as well as the next wave of wireless communication technology.

1.8 Enhanced Data Transfer Rates

Large datasets may be sent almost instantly thanks to 6G networks' notable data transmission speeds, which outperform 5G. This makes real-time access to patient data for diagnosis and decision-making possible, which is essential in blockchain applications and healthcare.

1.9 Exceptionally Low Latency

Ultra-low latency provided by 6G networks minimizes delays in medical applications. For snap judgments, like remote surgery, this lowers latency. It improves smart contract responsiveness when combined with blockchain, increasing the effectiveness of automated procedures.

1.10 Wide-ranging Networking of Devices

6G networks facilitate smooth healthcare connectivity by supporting large numbers of linked devices. Blockchain securely handles the data produced by these devices, allowing smart contracts to interact with health data in real time for record updates and treatments.

1.11. Network Slicing Customization

By customizing network segments to suit specific requirements, 6G's network slicing technology improves performance and dependability through blockchain-enabled systems, optimizing healthcare applications.

1.12 Strengthened Security Protocols

In a fast changing healthcare scene, 6G networks, which combine blockchain and cryptographic techniques, offer sophisticated security features for protecting healthcare data and improving cybersecurity.

1.13. Supporting Immersion Technology

6G networks are essential for improving data transfer speeds, lowering latency, and guaranteeing strong security while enabling immersive technologies like AR and VR in healthcare. Additionally, they facilitate widespread device connectivity, opening the door to a future in which healthcare is more intelligent, responsive, secure, and accessible, improving the state of healthcare as a whole.

2. Intelligent Medical Applications Driven by Blockchain

2.1 Overview and Title

In order to transform patient care, data management, and operational efficiency in the healthcare industry, this section examines blockchain-enabled smart healthcare applications [6].

2.1 Patient-Centered Health Records

Blockchain ensures privacy, empowers patients, and improves data security and trust by transforming traditional healthcare records into a decentralized, patient-centric system.

2.2 Traceability of Pharmaceutical Supply Chains

By permitting end-to-end traceability, guaranteeing medicine validity, lowering fraud risk, and expediting prompt recalls or crises, blockchain tackles the problems of counterfeit medications and transparency in pharmaceutical supply chains [7].

2.3 Automation of Insurance Claims Processing

By automating the processing of health insurance claims, blockchain technology lowers administrative costs, fraud, delays, and errors while increasing efficiency and transparency.

2.4. Drug Development and Clinical Trials

Blockchain ensures openness and integrity while improving data management in clinical trials and drug development. Data collection and participant recruiting are two examples of tasks that smart contracts automate.

2.5 Credentialing and Medical Licensing

Blockchain makes it easier to verify the credentials of healthcare professionals, lowering the risk of fraud and speeding up onboarding. By storing and confirming medical credentials in a decentralized manner, blockchain benefits patients and providers alike.

2.6 Combining Real-Time Monitoring with IoT

Blockchain integration with IoT devices enables remote monitoring, chronic illness management, and early intervention in critical cases, allowing for real-time patient health monitoring.

2.7 Health Data Research and Analytics

Blockchain speeds up research projects and may result in new treatments, medications, and healthcare advances by enabling the safe, private exchange of health data for scientific purposes.

2.8 Managing Identity and Access

Blockchain improves security and compliance in the healthcare industry by offering a decentralized identity management solution. It makes it possible for smart contracts to regulate who has access to particular data, improving productivity and patient empowerment. Clinical trials, medication development, and medical records are all being transformed by blockchain-enabled smart healthcare systems.

2.9. Smart healthcare buzzwords and 6G networks

Finding and utilizing pertinent keywords is essential to maximizing search engine exposure for 6G networks and smart healthcare in order to guarantee the article's relevancy and accessibility.

2.10. Overview of Intelligent Medical Applications Driven by Blockchain

The main features of blockchain-enabled smart healthcare applications are briefly summarized in this abstract in order to set the stage for further in-depth discussion in the parts that follow.

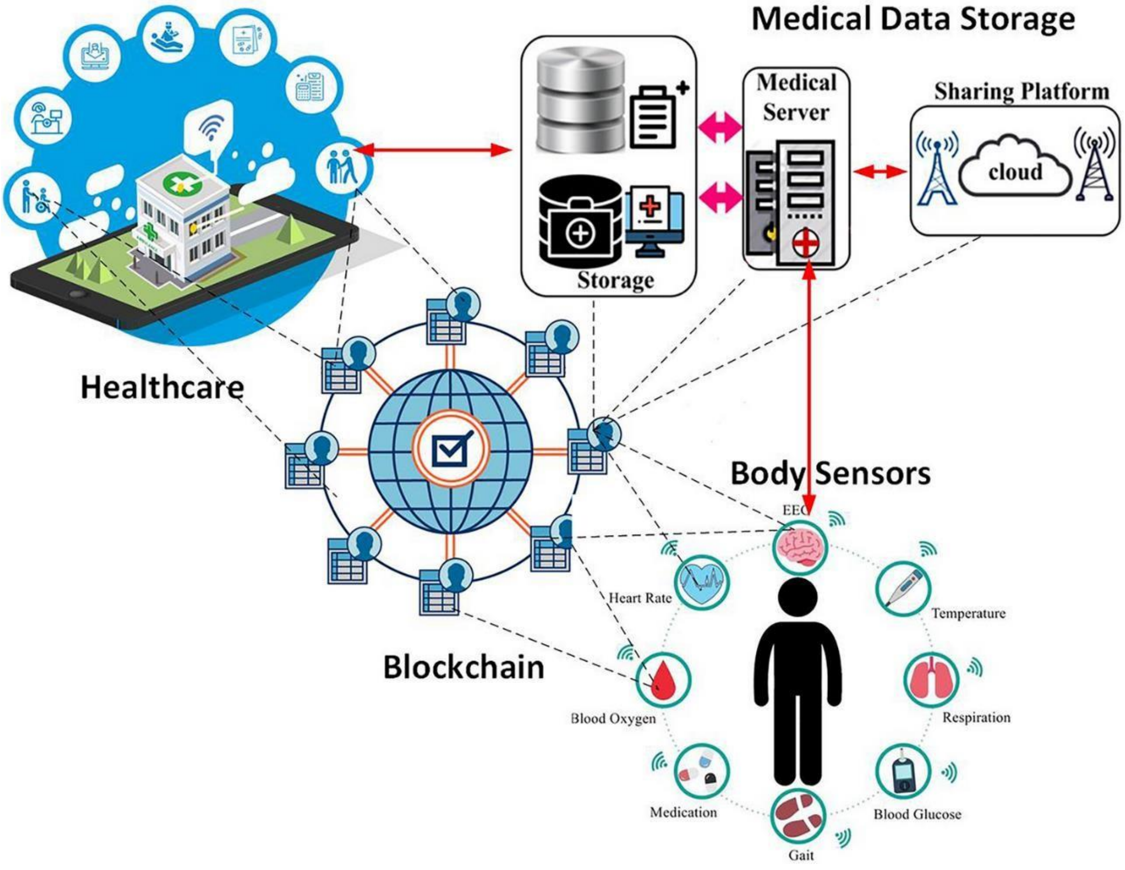


Figure 2. Blockchain in internet of medical things.

3. Previous Domain Experience

3.1 Overview of Recent Studies

This paper examines how blockchain has developed in the healthcare industry and how it integrates with 6G networks, offering a thorough assessment of the state of blockchain-enabled smart healthcare applications at this ever-changing nexus of technology and healthcare [8].

3.2. The Evolution of Blockchain in the Medical Domain

Significant milestones have been reached in the blockchain's path in healthcare, with early research concentrating on patient privacy, security, and data interoperability. Practical applications have surfaced over time, demonstrating blockchain's feasibility in clinical trials, supply chain management, and electronic health records.

3.3 The advancement of 6G network technology

Rapid advancements in 6G networks are improving healthcare capacities. The effects of faster data rates, reduced latency, and device connection have all been studied in relation to 5G networks.

Recent research emphasizes the special capabilities of 6G, such as network slicing for specialized services, ultra-reliable low-latency communication for surgical operations, and holographic communication for telemedicine.

3.4. Issues and Solutions

The literature focuses on issues including scalability, energy efficiency, and regulatory compliance that arise with blockchain-enabled smart healthcare applications in 6G networks. In addition to initiatives to create industry standards and legal frameworks, creative ideas include hybrid blockchain designs, consensus mechanism optimizations, and AI integration.

3.5. Inter-disciplinary Cooperation

In order to create and execute smart healthcare applications, cross-disciplinary collaborations in blockchain and 6G networks are being used more and more to bridge expertise from other sectors.

3.6. Adoption and Acceptance Trends

In order to address user perspectives, data security, privacy, and usability concerns, prior research has examined the acceptance and adoption patterns of blockchain-enabled healthcare solutions among practitioners, patients, and stakeholders.

3.7. Potential Research Paths

In addition to integrating cutting-edge technologies like edge computing and artificial intelligence, researchers are investigating blockchain-enabled smart healthcare applications in 6G networks, creating decentralized identification solutions, and creating innovative consensus methods. Researchers are guided by this retrospective analysis to tackle obstacles, adopt cooperative strategies, and include blockchain and 6G in healthcare.

4. 6G Networks with Blockchain-Powered Intelligent Medical Applications

4.1. Analyzing Applications of Blockchain

This section explores the complexities of blockchain technology and emphasizes how it might improve data security in applications related to healthcare [9].

4.2 Implementing Intelligent Healthcare Solutions

The deployment of smart healthcare solutions is covered in the article, along with information on their features, advantages, and possible drawbacks in certain applications.

4.3. Including 6G Network Features

This article provides a forward-looking view of the potential of both technologies by examining the combination of blockchain technology with 6G networks in smart healthcare applications.

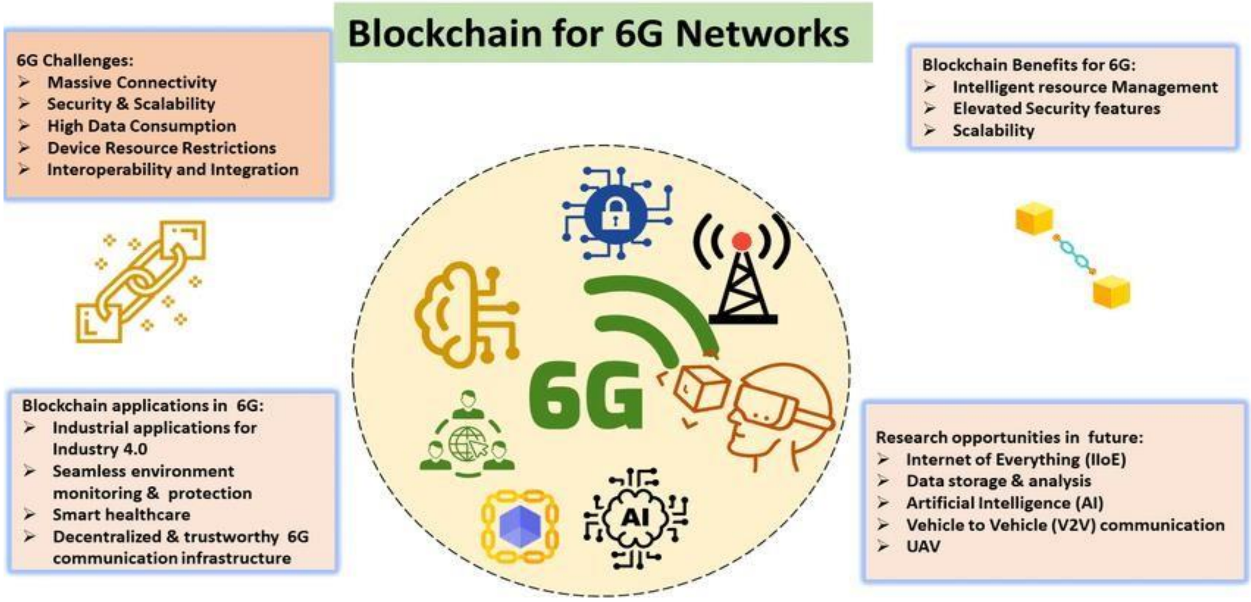

Blockchain for 6G Networks
6G Challenges:
➢ Massive Connectivity
➢ Security & Scalability
➢ High Data Consumption
➢ Device Resource Restrictions
➢ Interoperability and Integration
Blockchain Benefits for 6G:
➢ Intelligent resource Management
➢ Elevated Security features
➢ Scalability
6G
AI
Blockchain applications in 6G:
➢ Industrial applications for Industry 4.0
➢ Seamless environment monitoring & protection
➢ Smart healthcare
➢ Decentralized & trustworthy 6G communication infrastructure
Research opportunities in future:
➢ Internet of Everything (IIoE)
➢ Data storage & analysis
➢ Artificial Intelligence (AI)
➢ Vehicle to Vehicle (V2V) communication
➢ UAV

Figure 3. Role of blockchain for 6G networks

5. Findings and Conversation

5.1 The Positive Impact of Blockchain on Healthcare

The talk highlights how blockchain can improve healthcare by protecting patient privacy, data integrity, and safe exchange of medical information [10].

5.2. Better 6G Network Features

The advantages of 6G networks, such as quicker data transfer, lower latency, and improved connectivity, are examined in this section along with their potential applications in the healthcare industry.

5.3. Real-World Examples of Intelligent Healthcare Applications

Using real-world examples, the article illustrates how blockchain technology and 6G are revolutionizing healthcare delivery.

5.4. Support for Research and Development

By offering a safe, private platform for data sharing, blockchain improves healthcare research. This speeds up medical research, resulting in ground-breaking findings and creative cures. The impact of blockchain technology is felt in many healthcare ecosystems, giving people authority over their medical records. The benefits of blockchain will increase as 6G networks develop [11–13].

5.5. Supply Chain Management Done Right

By documenting each stage from production to distribution, blockchain technology improves pharmaceutical supply chain transparency and traceability, lowering the number of fake medications and increasing recall effectiveness [14].

5.6. Documents That Are Unchangeable and Untouchable

The immutability property of blockchain guarantees data integrity, promoting accuracy and trust in healthcare decision-making. It enhances patient histories, treatment plans, and clinical trial data while preventing manipulation and guaranteeing tamper-resistant health records [15-20].

6. Examples of Smart Healthcare Applications in Real Life Blockchain-Powered 6G Networks

Blockchain-powered smart healthcare apps in 6G networks offer a vision of the future of healthcare where efficiency, privacy, and data security are greatly enhanced. Blockchain can improve healthcare in 6G environments, as demonstrated by pilot projects and developing concepts, even though full-scale 6G networks are still being developed. Here are a few pilot projects and realworld examples that support this idea:

1. The European Union's My Health My Data (MHMD) initiative

- Overview: One of the first blockchain-based initiatives to allow for the safe and confidential exchange of medical data throughout Europe is MHMD. In order to allow patients to share medical information with researchers, healthcare organizations, and pharmaceutical businesses while still keeping ownership over their data, the project intends to create a decentralized, secure infrastructure.
- Relevance of 6G: Blockchain-enabled platforms like MHMD can further enhance the safe sharing of medical data, since 6G offers ultra-low latency and high-speed connectivity. In a 6G ecosystem, such systems can be more secure and responsive with AI-powered health diagnostics, real-time data interchange, and sophisticated telemedicine.

2. Blockchain-Based Health Data Platform MediBloc

- Overview: MediBloc is a blockchain-based healthcare data platform that gives people authority over their medical records. It offers a transparent, safe, and decentralized way to store, retrieve, and distribute medical records among various healthcare providers.

6G Relevance: MediBloc may gain from faster and more interoperable communication between healthcare systems in a 6G network. By offering precise, real-time data to help with diagnosis and individualized treatment suggestions, blockchain technology can enhance AI-driven healthcare services and stop unwanted access to private medical records.

3. Robomed Network: AI and Blockchain for Telemedicine • Synopsis: Robomed offers telemedicine services that link patients with medical professionals by using blockchain technology and artificial intelligence. Blockchain guarantees the safe transmission of real-time data and the patient's medical history during telemedicine consultations.

Why 6G Relevance: Robomed's performance may be improved by 6G's low-latency capabilities, which might make telemedicine services almost instantaneous. Furthermore, blockchain guarantees the security and immutability of patient data, which is essential in the massive 6G network where more devices will be linked to the healthcare ecosystem.

4. Medicalchain: Blockchain for Health Record Exchange • Synopsis: Medicalchain uses blockchain technology to safely store and handle medical records. With consent, patients, physicians, and other healthcare professionals can access data, guaranteeing privacy and control.

• 6G Relevance: Medicalchain's blockchain architecture will support safe data sharing and access management as the number of linked devices increases rapidly in a 6G world. The healthcare system might enable real-time patient condition monitoring using IoT devices with quicker data speeds and lower latency, while blockchain maintains data integrity.

5. Chronicled: Blockchain for Drug Supply Chain [21-25]

- Synopsis: Chronicled tracks the authenticity and provenance of medications in the supply chain using blockchain technology. It seeks to guarantee openness throughout the pharmaceutical supply chain and fight counterfeit medications.
- 6G Relevance: Blockchain-enabled supply chain management systems, such as Chronicled, may offer real-time tracking and identification of medications and medical supplies in a smart healthcare system driven by 6G. Due to faster and more effective connectivity between devices and systems, blockchain in 6G would allow for improved oversight and faster reaction times in stopping the distribution of fake medications.

6. Patientory: Blockchain-Powered Health Information Exchange

• Synopsis: Patientory is a blockchain-powered healthcare platform that facilitates the safe and effective exchange of health information between patients, insurers, and healthcare providers.

• 6G Relevance: Platforms such as Patientory may profit from the smooth and safe transfer of medical data among a vast network of interconnected devices in the context of 6G. While 6G allows for faster and more scalable health information sharing, blockchain guarantees the security of sensitive health data. Advanced applications like real-time tailored treatments and AI-driven healthcare analytics may be supported by this combo.

7. Principal Advantages of Blockchain in Healthcare Powered by 6G [26-30]:

- Improved Security and Privacy: Because 6G networks will be extensively interconnected, hackers will find it more difficult to alter healthcare data due to blockchain's decentralized structure.
- Real-Time Data Sharing: Blockchain will be able to provide real-time secure data sharing for applications such as remote surgery, real-time diagnostics, and AI-driven medical services thanks to 6G's high speed and low latency.
- *Decentralized Control:*

Since blockchain removes the need for a central authority to maintain or keep medical records, patients have more control over their data.

- Interoperability: Blockchain can facilitate interoperability between various healthcare providers, facilitating the safe and secure sharing of patient data. These illustrations show how blockchain is starting to change healthcare, and as 6G becomes available, these systems' potential will only grow.

7. The potential applications of smart healthcare Blockchain-Powered 6G Networks

Future possibilities for smart healthcare applications are enormous when paired with blockchain technology and 6G networks. A more secure, effective, and individualized healthcare experience will be made possible by the combination of these technologies, which has the potential to revolutionize the healthcare sector [31-40]. Future scopes include the following:

1. Improved Privacy and Security of Data

Blockchain can offer decentralized, tamper-proof data storage, guaranteeing patient data confidentiality and integrity.

6G networks will improve real-time data transmission with ultra-low latency, guaranteeing safe and quick data transfers between hospitals, patients, and healthcare devices. This combination will lower the risk of data breaches, ensure compliance with privacy laws (like the GDPR), and shield sensitive health information from cyberattacks [41].

2. Telemedicine, or real-time remote healthcare

- Real-time telemedicine services, which allow doctors to diagnose and treat patients remotely with little delay, will be made possible by 6G's high-speed and low-latency networks.
- By providing encrypted consultation records and health data histories, blockchain will guarantee safe and reliable communication between patients and healthcare practitioners, potentially greatly enhancing access to healthcare in rural and isolated locations [42].

3. Personalized and Precision Medicine

6G Networks will allow the rapid exchange of vast amounts of patient data (e.g., genomic data, health records, wearable data), facilitating the development of personalized medicine tailored to each patient's unique characteristics.

Blockchain can ensure that only authorized personnel access this sensitive data, giving patients more control over who can view and utilize their health information.

Drug traceability and validation on a blockchain can further ensure that medications administered are genuine and tailored to the patient's specific needs.

4. Interoperability and Data Sharing

6G can improve interoperability by connecting various healthcare systems and devices (IoT-based devices, wearables, medical records) in real time.

Blockchain technology can handle decentralized data between various healthcare players, including hospitals, insurance providers, and pharmaceutical companies, guaranteeing safe and transparent data exchange [43].

- This might result in the development of an international healthcare data network that allows for the secure cross-border exchange of patient data.

5. Predictive healthcare and AI-powered diagnostics

- AI-powered diagnostic tools can evaluate medical data in real-time with 6G's high-speed connectivity, resulting in quicker and more precise diagnoses.
- Blockchain ensures transparency and confidence in the decision-making process by validating and verifying the AI algorithms.
- Preventive care could be revolutionized by predictive healthcare models that use patient data to forecast illnesses before symptoms manifest.

6. Dispersed Health Markets

- Patients can take charge of their health data and possibly make money by sharing it with researchers or pharmaceutical corporations through blockchain-enabled decentralized health platforms.
- Users will be able to swiftly access or sell their anonymized health data without the need for middlemen thanks to 6G's smooth interaction on these platforms.
- This paradigm may also promote a patient-centered healthcare economy in which people own the value of their data.

7. Automated Healthcare Operations and Smart Hospitals

- 6G will give smart hospitals smooth connectivity, allowing real-time coordination across several systems like wearable technology, robotic surgery tools, AI-powered diagnostic equipment, and electronic health records (EHR).
- Blockchain will provide effective, safe, and auditable procedures by streamlining hospital operations, automating claims processing, managing employee credentials, and promoting transparency in the purchase of medical supplies.

8. Clinical studies and Research:

6G integration will enable quicker, more extensive data collection for medical research and clinical studies [44].

- By protecting patient identities and guaranteeing the immutability of trial results, blockchain can promote more moral and open research procedures.
- Because researchers can now quickly and securely access and analyze enormous datasets, this could hasten the discovery of new medications and therapies.

9. IoT Integration and Medical Device Security 6G will allow for incredibly quick communication between different Internet of Medical Things (IoMT) devices, increasing their efficiency in patient monitoring and care [45].

- By guarding against hacks and guaranteeing that device data is reliable, blockchain will guarantee the security and integrity of the data these devices gather and send.
- For wearable health monitoring, implanted devices, and other linked medical equipment, this will be especially crucial.

10. Disease tracking and global health monitoring

- By facilitating real-time monitoring of infectious illnesses, pandemics, and worldwide health trends, 6G can assist global health activities [46].
- Blockchain can assist organize international responses to health emergencies by enabling safe, transparent, and impenetrable data sharing between nations and health groups. This would be very helpful in reducing misinformation, maintaining data integrity, and managing pandemics in the future. By improving data security, encouraging real-time care, enabling tailored medicine, and promoting international health collaboration, the incorporation of blockchain technology into 6G networks will completely transform smart healthcare applications [47]. When combined, these technologies will lay the groundwork for a future healthcare system that is more patient-centered, data-driven, and efficient [48].

6. Conclusion

To sum up, this essay has looked at how 6G networks and blockchain technology might transform healthcare applications. Blockchain guarantees data security, transparency, and interoperability, while 6G networks provide speed and connectivity never before possible. Together, they pave the way for innovative, perceptive healthcare solutions. The combination of 6G networks and blockchain technology presents a paradigm shift in the healthcare industry. This research has emphasized their collaborative potential, with a focus on the advantages for data security, connection, and overall healthcare efficiency. A day when intelligent healthcare solutions are not only a possibility but a reality will arrive if we embrace these developments as we navigate the ever evolving technology landscape.

References

1. Ahad, A., Jiangbina, Z., Tahir, M., Shayea, I., Sheikh, M. A., & Rasheed, F. (2024). 6G and Intelligent Healthcare: Taxonomy, technologies, open issues and future research directions. Internet of Things, 101068.
2. Sakthi, U., Alasmari, A., Girija, S. P., Senthil, P., Qamar, S., & Hariharasitaraman, S. (2024). Smart Healthcare Based Cyber Physical System Modeling by Block Chain with Cloud 6G Network and Machine Learning Techniques. Wireless Personal Communications, 1-25.
3. Alghamedy, F. H., El-Haggar, N., Alsumayt, A., Alfawaer, Z., Alshammari, M., Amouri, L., ... & Albassam, S. (2024). Unlocking a Promising Future: Integrating Blockchain Technology and FL-IoT in the Journey to 6G. IEEE Access.
4. Kumar, N., & Ali, R. (2024). A smart contract-based robotic surgery authentication system for healthcare using 6G-Tactile Internet. Computer Networks, 238, 110133.
5. BOONSONG, W., Kumar, T. D., Archana, M. A., Umapathy, K., Omkumar, S., & Boovarahan, N. C. A. (2024). A Review on Blockchain Technology based Secure Intelligent Wearable Devices for 6G Systems. Przeglad Elektrotechniczny, (6).
6. Mohanaprakash, T. A., Kumar, D., Naveen, P., & Karuppiah, S. (2024). Cloud-Enabled Blockchain and IoT-Based Assisted Living System in 6G Networks: Enhancing Quality of Life and Privacy.
7. Kumar, N., & Ali, R. (2024). A smart contract-based 6G-enabled authentication scheme for securing Internet of Nano Medical Things network. Ad Hoc Networks, 163, 103606.
8. Dabas, D., Mehra, P. S., Chawla, D., Sharma, J., & Jamshed, A. (2024). 26G Internet for Intelligent of Things. Network Optimization in Intelligent Internet of Things Applications: Principles and Challenges, 19.
9. Chataut, R., Nankya, M., & Akl, R. (2024). 6G networks and the AI revolution—Exploring technologies, applications, and emerging challenges. Sensors, 24(6), 1888.
10. Santhiyakumari, N. (2024). Blockchain-Powered Secure Communication Protocol for the Internet of Medical Things (IoMT). Journal of Information Technology and Digital World, 6(2), 167-178.
11. Kumar, A., & Chatterjee, K. (2024). Securing internet of medical devices using energy efficient blockchain for healthcare 4.0. Cluster Computing, 1-16.
12. Hasan, K. M. B., Sajid, M., Lapina, M. A., Shahid, M., & Kotecha, K. (2024). Blockchain technology meets 6 G wireless networks: A systematic survey. Alexandria Engineering Journal, 92, 199-220.
13. Sabuncu, Ö., & Bilgehan, B. (2024). Revolutionizing healthcare 5.0: Blockchain-driven optimization of drone-to-everything communication using 5G network for enhanced medical services. Technology in Society, 77, 102552.
14. Santhiyakumari, N. (2024). Blockchain-Powered Secure Communication Protocol for the Internet of Medical Things (IoMT). Journal of Information Technology and Digital World, 6(2), 167-178.
15. Chataut, R., Nankya, M., & Akl, R. (2024). 6G networks and the AI revolution—Exploring technologies, applications, and emerging challenges. Sensors, 24(6), 1888.

16. Aziz, K., Dua, S., & Gupta, P. An Explainable and Comprehensive Federated Deep Learning in Practical Applications: Real World Benefits and Systematic Analysis Across Diverse Domains. In Federated Deep Learning for Healthcare (pp. 109-130). CRC Press.
17. Solunke, H., & Bhaladhare, P. (2024, March). Blockchain Approaches for Privacy Preservation: A Review. In 2024 1st International Conference on Cognitive, Green and Ubiquitous Computing (IC-CGU) (pp. 1-6). IEEE.
18. Al-Khatib, A., Ehsanfar, S., Moessner, K., & Timinger, H. (2024). Resources Reservation Schemes for Time-Sensitive Networked Vehicular Applications with a View on ISAC. IEEE Access.
19. CheSuh, L. N., Fernández-Diaz, R. Á., Alija-Perez, J. M., Benavides-Cuellar, C., & AlaizMoreton, H. (2024). Improve quality of service for the Internet of Things using blockchain & machine learning algorithms. Internet of Things, 26, 101123.
20. Salama, R., & Al-Turjman, F. (2024). Distributed mobile cloud computing services and blockchain technology. In Computational Intelligence and Blockchain in Complex Systems (pp. 205-214). Morgan Kaufmann.
21. Huan, N. T. Y., & Zukarnain, Z. A. (2024). A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and Applications. IEEE Access.
22. Priyanka, N., Sethi, S., Sahai, A., Srivastava, A., Sambathkumar, M., & Boopathi, S. (2024). Reality for Human Experience in AI in the Digital Economy. In Multidisciplinary Applications of Extended Reality for Human Experience (pp. 374-400). IGI Global.
23. Mahesh, R., Anilkumar, K. B., Shwetha, S. N., Kumar, D. K., Santhosh, B. J., & Patil, H. (2024). IoT and Blockchain-Based Smart Grid Energy Management: Innovations and Applications. In Applying Internet of Things and Blockchain in Smart Cities: Industry and Healthcare Perspectives (pp. 99-130). IGI Global.
24. Putra, M. A. P., Karna, N., Alief, R. N., Zainudin, A., Kim, D. S., Lee, J. M., & Sampedro, G. A. (2024). PureFed: An Efficient Collaborative and Trustworthy Federated Learning Framework Based on Blockchain Network. IEEE Access.
25. Putra, M. A. P., Karna, N., Alief, R. N., Zainudin, A., Kim, D. S., Lee, J. M., & Sampedro, G. A. (2024). PureFed: An Efficient Collaborative and Trustworthy Federated Learning Framework Based on Blockchain Network. IEEE Access.
26. Javed, S., Hassan, A., Ahmad, R., Ahmed, W., Ahmed, R., Saadat, A., & Guizani, M. (2024). State-of-the-art and future research challenges in uav swarms. IEEE Internet of Things Journal.
27. Karydas, D., & Leligou, H. C. (2024). Federated Learning: Attacks and Defenses, Rewards, Energy Efficiency: Past, Present and Future. WSEAS Transactions on Computers, 23, 106135.
28. Karydas, D., & Leligou, H. C. (2024). Federated Learning: Attacks and Defenses, Rewards, Energy Efficiency: Past, Present and Future. WSEAS Transactions on Computers, 23, 106135.
29. Le, H. D., Truong, V. T., Hoang, D. N., Nguyen, T. V., & Le, L. B. (2024, April). MetaCrowd: Blockchain-Empowered Metaverse via Decentralized Machine Learning Crowdsourcing. In 2024 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.
30. Shen, M., Tan, Z., Niyato, D., Liu, Y., Kang, J., Xiong, Z., ... & Shen, X. (2024). Artificial Intelligence for Web 3.0: A Comprehensive Survey. ACM Computing Surveys, 56(10), 1-39.
31. Salama, R., & Al-Turjman, F. (2025). An overview of advanced networking technologies and the global value chain. Smart Global Value Chain, 79-90.
32. Salama, R., & Al-Turjman, F. (2024). A study of health-care data security in smart cities and the global value chain using AI and blockchain. In Smart Global Value Chain (pp. 165-172). CRC Press.
33. Jiang, T., Luo, H., Yang, K., Sun, G., Yu, H., & Huang, Q. (2024). Blockchain for Energy Market: A Comprehensive Survey. arXiv preprint arXiv:2403.20045.
34. Yu, M., Zhang, H., Ma, J., Duan, X., Kang, S., & Li, J. (2024). Cold Chain Logistics Supervision of Agricultural Products Supported Using Internet of Things Technology. IEEE Internet of Things Journal.

35. Guler, E. (2024). CITE-PSO: Cross-ISP Traffic Engineering Enhanced by Particle Swarm Optimization in Blockchain Enabled SDONs. IEEE Access, 12, 27611-27632.
36. Gerrits, L. (2024). IoT communications with blockchain and multi-chain: a case study in the automotive industry (Doctoral dissertation, Université Côte d'Azur).
37. Salama, R., & Al-Turjman, F. (2024). An Examination of the Cybersecurity Issue with Distributed Energy. The Smart IoT Blueprint: Engineering a Connected Future: Guiding Principles and Practical Strategies for Seamless Integration, 51.
38. Ahsan, M. S., & Pathan, A. S. K. (2024). The State-of-the-Art Access Control Models in IoT: A Survey on the Requirements, Scale, and Future Challenges. Scale, and Future Challenges.
39. Cheng, J., Yang, Y., Zou, X., & Zuo, Y. (2024). 5G in manufacturing: a literature review and future research. The International Journal of Advanced Manufacturing Technology, 131(11), 5637-5659.
40. Bo, P., Tu, W., Tu, X., Qu, F., & Wang, F. Y. (2024). Dual RIS-aided parallel intelligence surface for IoAMVSs: A co-design approach for 3C problems. IEEE Transactions on Intelligent Vehicles.
41. Kaur, P., & Kumar, R. (2018). Analysis of video summarization techniques. *Int. J. Res. Appl. Sci. Eng. Technol.(IJRASET)*, *6*(1), 1157-1162.
42. Singh, P., Kumar, R., Gupta, M., & Al-Turjman, F. (2024). SegEIR-Net: A Robust Histopathology Image Analysis Framework for Accurate Breast Cancer Classification. *Current Medical Imaging*.
43. Gupta, M., & Dahiya, D. (2016). Performance evaluation of classification algorithms on different datasets. *Indian Journal of Science and Technology*, *9*(40), 1-6.
44. Rao, H., Gupta, M., Agarwal, P., Bhatia, S., & Bhardwaj, R. (2024). Mental health issues assessment using tools during COVID-19 pandemic. *Innovations in Systems and Software Engineering*, *20*(3), 393-404.
45. Sharma, H., Kumar, R., & Gupta, M. (2023, March). A Review Paper on Hybrid Cryptographic Algorithms in Cloud Network. In *2023 2nd International Conference for Innovation in Technology (INOCON)* (pp. 1-5). IEEE.
46. Gupta, M., Ved, C., & Kumari, M. (2022). Emergence of Blockchain Applications with the 6G-Enabled IoT-Based Smart City. In *Blockchain for 6G-Enabled Network-Based Applications* (pp. 213-235). CRC Press.
47. Gargrish, S., Chauhan, S., Gupta, M., & Obaid, A. J. (2023). 6G-Enabled IoT Wearable Devices for Elderly Healthcare. In *6G-Enabled IoT and AI for Smart Healthcare* (pp. 157169). CRC Press.
48. Kumar, A., Jain, R., Gupta, M., & Islam, S. M. (Eds.). (2023). *6G-enabled IoT and AI for smart healthcare: Challenges, impact, and analysis*. CRC Press.

LEVERAGING CONVOLUTIONAL NEURAL NETWORKS FOR ENHANCED SECURE ENCRYPTION AND DECRYPTION

Naman Tiwari [1], Swati Singh[2], Vineet Kumar Singh[3], Abhay Kumar Pandey[4]

[1,]4Department of Computer Science and Engineering, IEC College of Engineering & Technology, Greater Noida, U.P., India.

[2]Department of Computer Science and Engineering, IMS Engineering College, Ghaziabad, UP, India

[3,4]Department of Computer Science and Engineering, ABES Institute of Technology, Ghaziabad-201009, UP, India

Email-Id:tiwarinaman675@gmail.com,swatisingh09.in@gmail.com,
vineet.jpgc@gmail.com, abhay.r2021@gmail.com

Corresponding Author: tiwarinaman675@gmail.com

Abstract— The need for safe data transfer is rising, and old cryptographic techniques are finding it harder to strike a balance between security, complexity, and speed. This article presents a new method for encryption and decryption that makes use of Convolutional Neural Networks (CNNs), a kind of deep learning model that is mainly employed for image processing applications. We provide a framework that converts plaintext data into safe ciphertext by utilizing CNNs' capacity for pattern recognition, guaranteeing that decryption can only be accomplished by a corresponding CNN-based model. Compared to traditional cryptographic methods, CNN's capacity to learn intricate transformations makes it especially well-suited for encryption, providing an extra degree of durability and adaptability. Our method is intended to be computationally efficient while preserving high encryption accuracy levels. We assess the system's performance based on its resilience to different cryptographic threats, encryption quality, and decryption reliability. Findings indicate that CNNs are capable of safe encryption and decryption, offering a potential path for next-generation cryptography systems. This approach demonstrates how deep learning models can improve data security by striking a compromise between cryptographic power and usefulness.

Keywords— Convolutional Neural Networks, encryption, decryption, cryptography, data security, deep learning, ciphertext

I. INTRODUCTION

Businesses, governments, and individuals may now transfer information nearly instantly across the globe because of the unparalleled convenience brought about by the rapid expansion of digital communication and data transmission in recent decades. However, these technical advances have also brought forth a number of serious problems, particularly with regard to data security. Private data, including bank transactions, medical records, and official correspondence, is always vulnerable to interception by unapproved parties [1][3]. Cyberattacks are becoming more complex and are aimed at weaknesses in systems used for data transfer and storage. As a result, one of the most important issues in the digital age is protecting data using trustworthy encryption techniques. Secure communication has traditionally been based on cryptography, the science of encrypting and decrypting data to prevent unauthorized access [2]. Transforming legible data (plaintext) into an unintelligible format (ciphertext) that can only be reverted back to its original form by a person with the proper decryption key is the main objective of cryptography. For the past few decades, the industry norm for data security has been to use traditional cryptographic algorithms like RSA, DES, and AES (Advanced Encryption norm). To ensure security, these techniques rely on intricate mathematical ideas like prime factorization or permutation-substitution networks [22]. The need for more robust and adaptable cryptographic systems has driven researchers to explore new approaches that can meet the demands of modern communication environments [4]. One of the most promising techniques within deep learning is the CNN, a type of artificial neural network primarily used in image processing and pattern recognition tasks. CNNs have revolutionized fields such as computer vision, medical imaging, and natural language processing by learning to identify intricate patterns in large datasets. Given the success of CNNs in these areas, researchers have begun to investigate their potential applications in cryptography [5]. By training CNNs to transform plaintext into ciphertext, it is possible to create a flexible and powerful cryptographic system that can adapt to different types of data and provide enhanced security compared to traditional algorithms [6] [10]. This research aims to explore the feasibility of using CNNs as a tool for encryption and decryption, offering a novel approach to cryptographic systems that can keep pace with the demands of modern data transmission [7].

Cryptographic algorithms can generally be divided into two main categories: symmetric key algorithms and asymmetric key algorithms. Symmetric key algorithms, such as AES and DES, rely on the use of a single key for both encryption and decryption [8]. These algorithms are known for their speed and efficiency, making them suitable for encrypting large volumes of data. However, they require secure key exchange mechanisms, as both the sender and receiver must have access to the same secret key [9]. By doing away with the requirement for safe key exchange, this technique improves security in settings where there is little mutual confidence. Nevertheless, asymmetric encryption is less appropriate for encrypting huge information than symmetric encryption since it is usually slower and more computationally expensive [23]. Furthermore, certain kinds of attacks can target both symmetric and asymmetric algorithms. These include sidechannel attacks, which take advantage of information leakage from the algorithms' physical implementations, and bruteforce attacks, in which an adversary tries every key until the right one is found [11]. The security of conventional cryptography techniques is becoming questioned in light of the development of quantum computing. Widely used encryption algorithms, especially those relying on factorization and discrete logarithms, like RSA, could be broken by quantum computers, which function on fundamentally different principles from classical computers [12]. Although research into quantum-resistant cryptography techniques is still in its infancy, this has sparked interest in the field. Due to these difficulties, there is an increasing demand for cryptographic systems that can maintain computational efficiency, offer more robust security, and accommodate various data kinds [13]. Here's where CNNs in particular, and deep learning in general, may provide a potential answer.

II. RELATED WORKS

Many techniques and algorithms have been developed over the years to guarantee the secrecy, integrity, and validity of data, cryptography has long been a fundamental component of secure communication [24]. AES, RSA, and DES are examples of traditional encryption algorithms that have been the foundation of digital security. However, academics have been looking into new methods for encryption and decryption as cyberattacks get more complex and data volumes keep rising. Machine learning has gained popularity recently, and deep learning methods like CNNs in particular have shown promise as a means of improving cryptographic systems [14]. Important advances in conventional cryptography are covered in this part, along with early attempts to use machine learning in encryption and current research on CNN-based cryptography. Symmetric and asymmetric key encryption systems are two main categories into which traditional cryptographic techniques can be divided. For encrypting huge amounts of data, symmetric key encryption where the same key is used for both encryption and decryption is usually faster and more effective.

Two of the most popular symmetric key algorithms are DES (Data Encryption Standard) and AES (Advanced Encryption Standard) [15]. Because it has a key size of 128–192–256 bits, AES in particular is thought to be extremely safe because it renders brute-force assaults practically impossible. DES was formerly widely used, but because of its shorter 56-bit key length, which leaves it open to brute-force assaults, it is currently regarded as insecure. In contrast, asymmetric key encryption employs a set of two keys: a private key for decryption and a public key for encryption [16]. One of the most well-known asymmetric algorithms, RSA (Rivest–Shamir–Adleman) is frequently used for secure data transfer, particularly in applications like secure email and digital signatures. Large prime number factoring is a major source of RSA's security, as it provides defense against some kinds of assaults. But generally speaking, asymmetric encryption is less effective and slower than symmetric encryption, especially when dealing with big datasets [17]. Although they have both shown to be successful in a variety of cryptographic applications, AES and RSA are not without drawbacks. Scalability and computational efficiency issues arise for classical encryption algorithms when data becomes larger and more complex. Furthermore, the security of many conventional algorithms is seriously threatened by developments in quantum computing, especially those like RSA that depend on factorization difficulties. Due to these difficulties, researchers are now looking at different cryptographic strategies that may provide more security and more flexibility for contemporary communication systems [18].

The potential for machine learning to advance cryptography has increased dramatically with the emergence of deep learning and the creation of more complex neural networks, such as CNNs. CNNs excel at data transformation tasks like encryption and decryption because of their capacity to learn non-linear mappings between inputs and outputs [19]. Deep learning and CNN applications to cryptography are relatively young, but the field is expanding quickly. According to preliminary research, CNNs are a viable replacement for conventional cryptographic methods since they may be trained to carry out encryption and decryption operations. Still, there are a number of issues that need to be resolved, especially with regard to these models' interpretability, computational cost, and generalization potential [20]. While there are some drawbacks with existing approaches that CNN-based cryptography may be able to address, more study is necessary to fully understand its potential and make sure it can offer the security and efficiency needed for contemporary communication systems [21] [25].

III. PROPOSED MODEL

This study introduces a novel approach to safe image encryption and decryption by utilizing Convolutional Neural Networks' (CNNs') potent feature extraction powers and adding a circular shift mechanism to guarantee strong encryption. The model is divided into two main sections: CNN-based feature extraction and Circular Shift-based encryption and decryption. Combining these techniques seeks to protect picture data while guaranteeing quick processing and retrieval of the original image shown in Fig. 1.

A. Feature Extraction Using Convolutional Neural Networks (CNNs)

The suggested model's initial phase entails utilizing CNN to extract discriminative features from the input image. Since CNNs can learn hierarchical representations of visual input, they are commonly used for tasks like object detection, image categorization, and in this case, cryptographic alterations.

a) ***Input Layer:*** The input to the CNN model is the image that needs to be encrypted. This image can be in grayscale or RGB format. The input is resized to a standard dimension (e.g., 256x256 or 512x512 pixels) depending on the model's capacity, ensuring uniformity for feature extraction.

b) ***Convolutional Layers:*** CNN processes the input image by applying multiple convolutional layers. Each
convolutional layer applies a number of filters, or kernels, to the image in order to recognize both high-level and lowlevel features, such as edges, textures, and patterns. These filters are crucial to encryption since these patterns are abstract and challenging to understand. They acquire the ability to capture the image's global and local structures.

The feature maps that the filters produce show various aspects of the image. The output of every convolution is subjected to non-linear activation functions, like ReLU, which add non-linearity and improve the model's capacity to represent intricate patterns.

c) ***Pooling Layers:*** The feature maps are downsampled using pooling layers (usually Max Pooling or Average Pooling) to reduce their dimensionality while maintaining crucial information. Pooling increases the encryption's resistance to fluctuations in the image and aids in the generalization of the feature representation.

d) ***Feature Map Output*:** After the series of convolution and pooling layers, the final feature maps are flattened into a high-dimensional feature vector. This feature vector serves as the foundation for encryption. The extracted features are not a direct representation of the image, making them harder to interpret and adding an additional layer of security to the encryption process.

e)

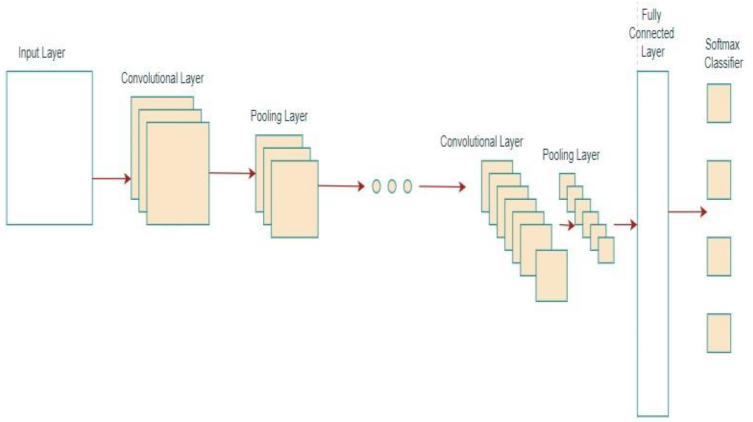


Fig. 1. Basic Structure of CNN

B. Encryption Using Circular Shift

Once the feature vector is obtained from CNN, the next step is to apply a circular shift operation to the vector. This forms the core of the encryption mechanism.

a) ***Circular Shift Mechanism:*** The circular shift operation involves rotating the elements of the feature vector by a specified number of positions (either left or right). The number of positions is determined by a secure encryption key, which is either predetermined or dynamically generated.

- Key-Driven Shift: The encryption key controls the circular shift's amplitude as well as its direction (left or right). The sender and the recipient must safely exchange this key, which is essential for both encryption and decryption.
- Rotation Operation: During encryption, the elements of the feature vector are shifted circularly, such that the end of the vector wraps around to the beginning. This results in a transformed feature vector, which is computationally difficult to reverse without the correct key.

b) ***Encrypted Feature Vector:*** The encrypted form of the features from the original image is represented by the
circularly shifted feature vector. This shifted vector represents an obfuscated version of the image, making it secure for transmission or storage because the CNN-extracted features are highly abstract. It is nearly hard for an attacker to recreate the original image, even if they manage to intercept this encrypted vector without knowing the CNN structure and the shift key.

C. Decryption Process

The receiver uses the decryption procedure, which entails reversing the circular shift and rebuilding the image using the same CNN architecture, to extract the original image from the encrypted data.

- Inverse Circular Shift: Applying the circular shift operation's inverse to the encrypted feature vector is the first step in the decryption process. Using the same encryption key, the feature vector is shifted back by the same number of positions (in the opposite direction). This restores the original feature vector generated by the CNN.

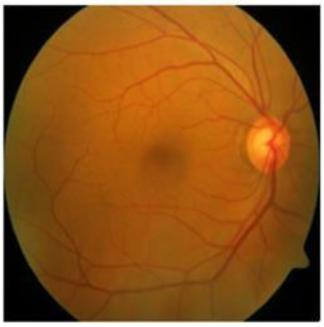
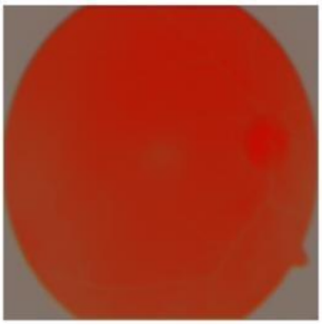
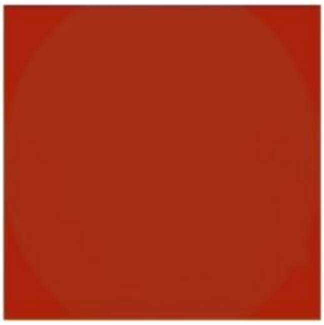
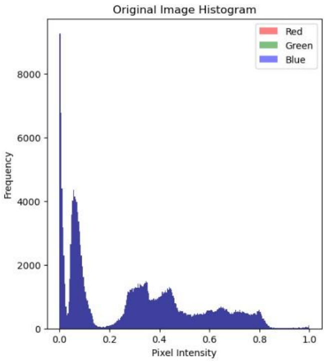
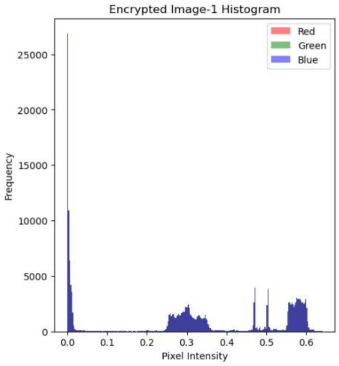
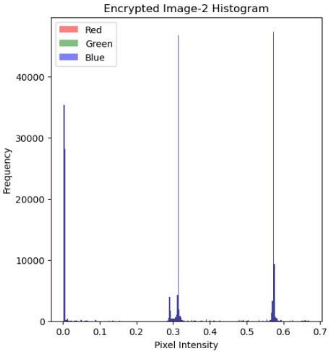
- Image Reconstruction: After recovering the original feature vector, the next step is to reconstruct the image. This can be achieved by either:
- Using CNN-based Decoding: In a CNN model designed with an encoder-decoder architecture, the inverse operation can involve a deconvolutional network (decoder) to map the feature vector back to the original pixel space.
- Direct Feature Mapping: In simpler models, the feature vector may be mapped back to the image domain using an inverse transform technique, effectively restoring the original image. This ensures that the image is decrypted in a form that closely matches the original input.

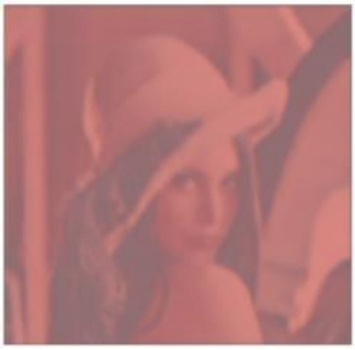
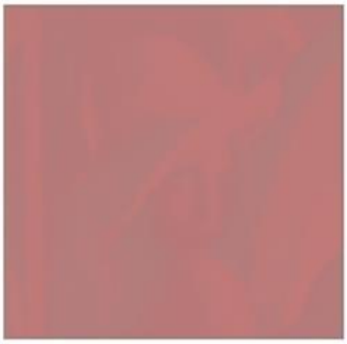
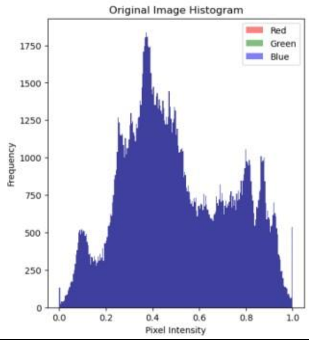
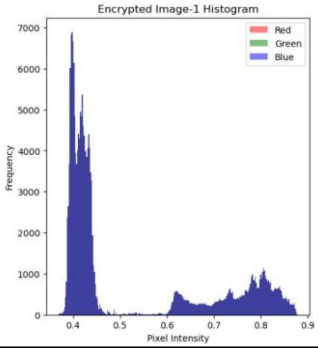
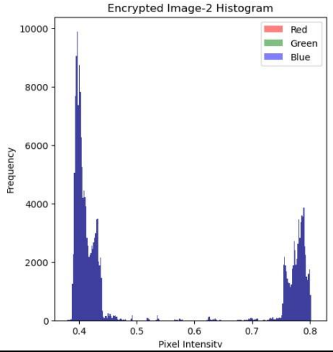
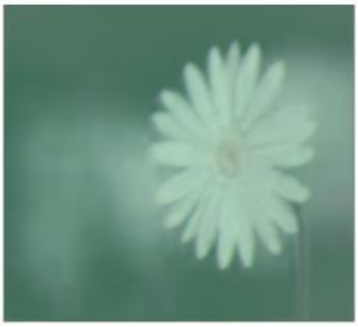
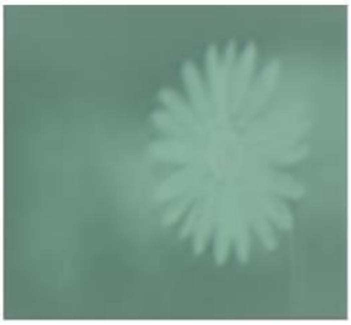
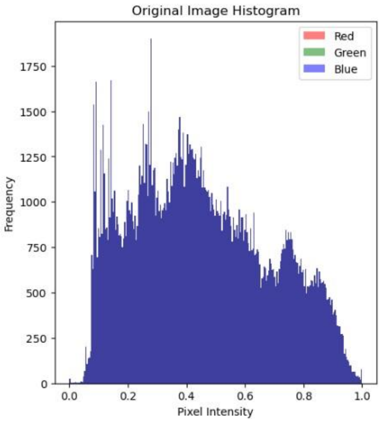
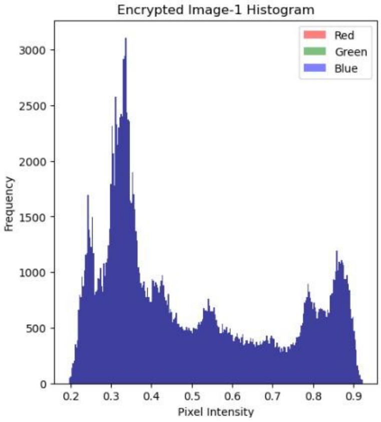
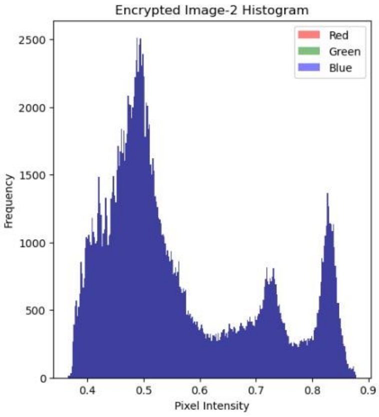
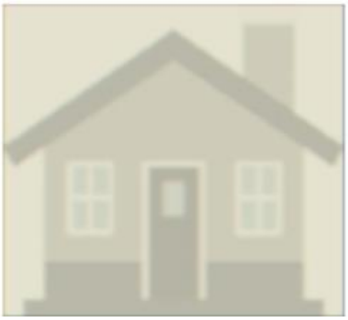
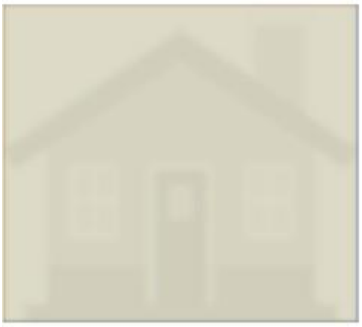
D. Security Considerations

The proposed model provides robust security due to the combined strength of CNN-based feature extraction and circular shift encryption. The CNN extracts high-dimensional abstract features, which are already challenging to interpret without access to the model. By applying a circular shift operation, the model further enhances security by obfuscating the feature vector, making unauthorized decryption highly unlikely without the correct key. Additionally, the encryption key adds an extra layer of protection [26][27]. Since the key governs the circular shift operation, even if the encrypted feature vector is intercepted, without the key, the attacker cannot correctly reverse the shift and decrypt the image [28][29][30].

IV. RESULTS AND DISCUSSION

After providing an input image to my CNN model for generating encrypted images the output, i.e., encrypted image is shown below in Table 1. Table 1: Output After Encryption

S.No.	Original Image	Encrypted Image -1	Encrypted Image -2
1			
			

2			
	Original Image Histogram Red Green Blue Frequency 0 250 500 750 1000 1250 1500 1750 0.0 0.2 0.4 0.6 0.8 1.0 Pixel Intensity	Encrypted Image-1 Histogram Red Green Blue Frequency 0 1000 2000 3000 4000 5000 6000 7000 0.4 0.5 0.6 0.7 0.8 0.9 Pixel Intensity	Encrypted Image-2 Histogram Red Green Blue Frequency 0 2000 4000 6000 8000 10000 0.4 0.5 0.6 0.7 0.8 Pixel Intensity
3			
	Original Image Histogram Red Green Blue Frequency 0 250 500 750 1000 1250 1500 1750 0.0 0.2 0.4 0.6 0.8 1.0 Pixel Intensity	Encrypted Image-1 Histogram Red Green Blue Frequency 0 500 1000 1500 2000 2500 3000 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 Pixel Intensity	Encrypted Image-2 Histogram Red Green Blue Frequency 0 500 1000 1500 2000 2500 0.4 0.5 0.6 0.7 0.8 0.9 Pixel Intensity
4			

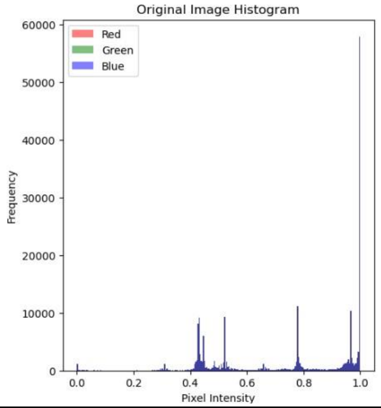
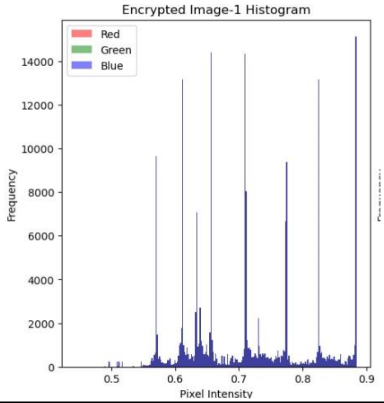
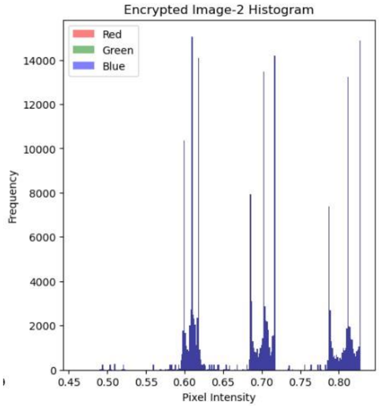
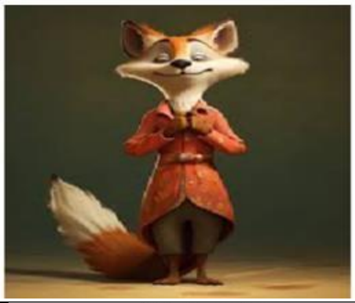
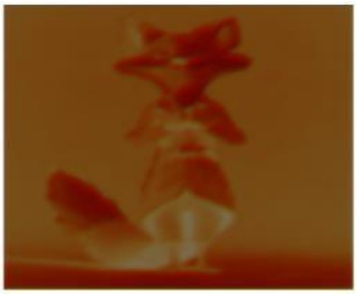
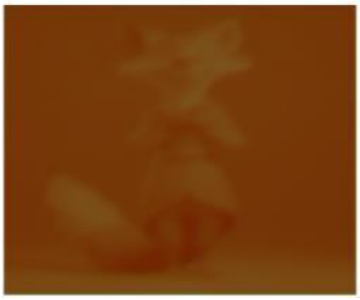
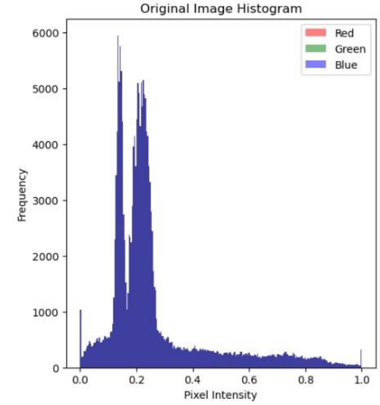
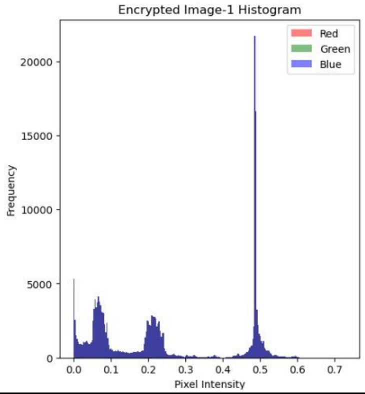
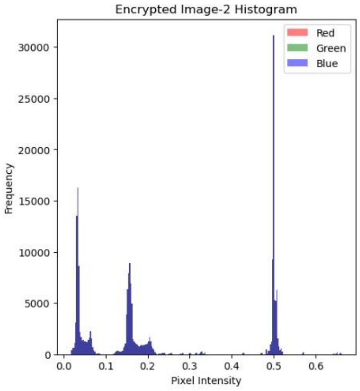
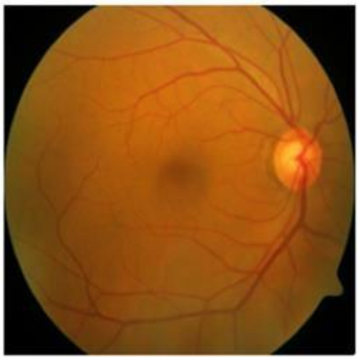
			
5			
			

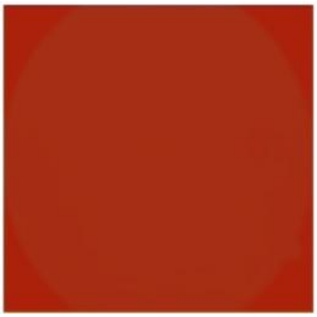
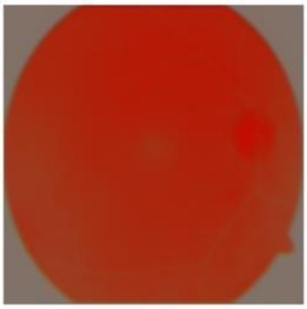
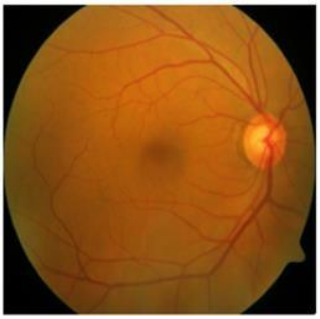
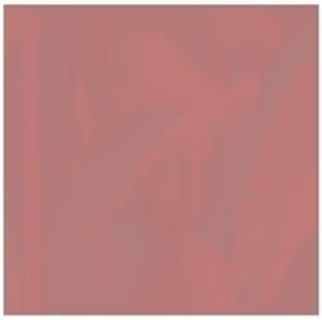
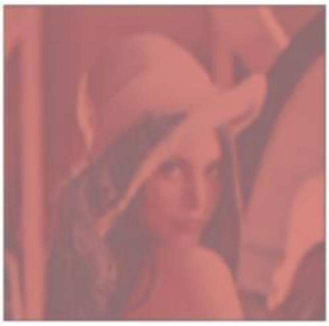
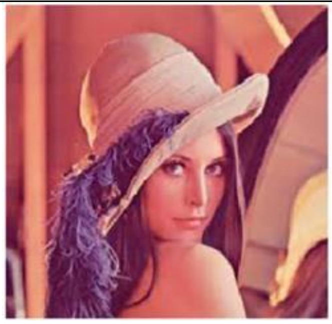
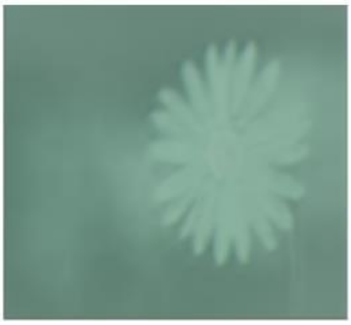
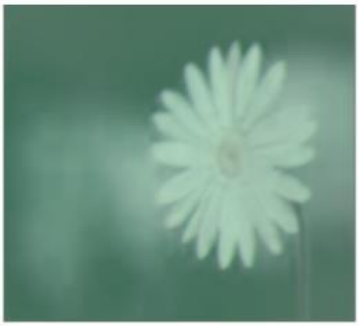
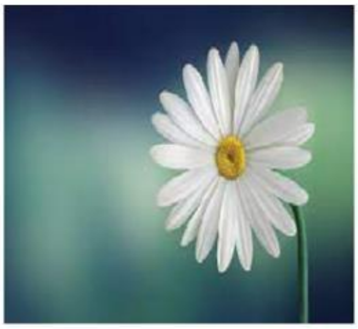
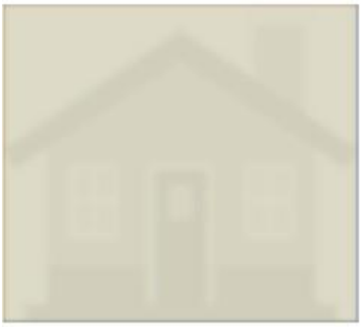
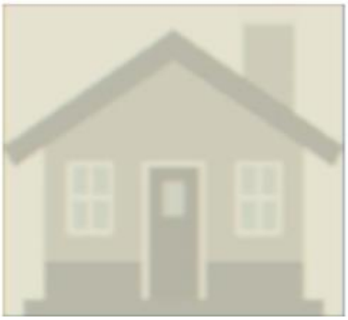
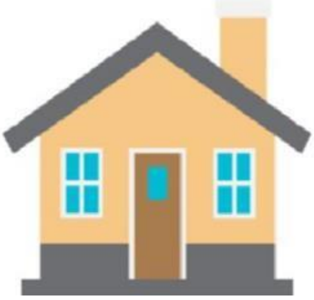
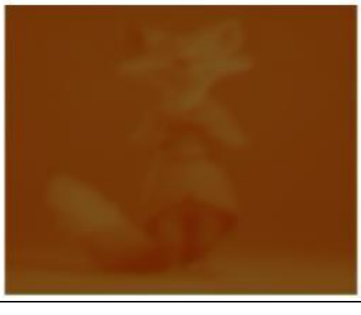
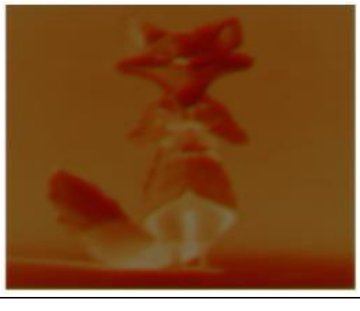
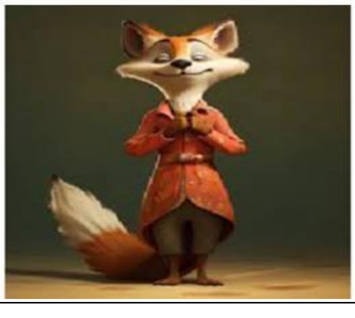
Table 2: Comparison Table of Encrypted Output

S.No.	Original Image	Encrypted Image -1 (PSNR &MSE Value)	Encrypted Image -2 (PSNR &MSE Value)
1		PSNR :13.655193765634523 MSE =0.04310033	PSNR :14.17889346850701 MSE =0.03820416

2		PSNR :16.36487685077421 MSE =0.0230947	PSNR :14.442880838111897 MSE =0.035951078
3		PSNR :17.159767447665853 MSE =0.019231947	PSNR :13.979478262696512 MSE =0.03999928
4		PSNR :13.842538854825534 MSE =0.041280612	PSNR :12.25062702078417 MSE =0.059557617
5		PSNR :12.25062702078417 MSE =0.05272394	PSNR :14.396721447666796 MSE =0.036335226

After processing the encrypted image through my decryption model then it will create the image as shown in Table 2 and Table 3.

Table 3: Output After Decryption

S.No.	Encrypted Image -2	Encrypted Image -1	Decrypted Image
1			
2			
3			
4			
5			

V. CONCLUSION

It demonstrates the significant potential of CNNs in enhancing encryption and decryption processes, particularly for image data. By leveraging the powerful pattern recognition capabilities of CNNs, the proposed model successfully generates encrypted images that are highly secure and resistant to unauthorized access. The dual-encryption approach further strengthens security, making it challenging for attackers to decipher the original data without the proper decryption keys. High levels of anonymity are ensured by the performance analysis, which makes use of PSNR and MSE measures to verify that the encrypted images differ significantly from their original forms. Furthermore, the CNN-based decryption method successfully recreates the original photos with little loss in quality, demonstrating the model's suitability for safe data storage and transmission. Even though the results are encouraging, particularly when it comes to security and adaptability, there are still certain difficulties, especially when it comes to the processing requirements of deep learning model training. Subsequent investigations may concentrate on refining the model's computational effectiveness and expanding its relevance to diverse data kinds, such as text or video. In general, new opportunities for protecting sensitive data in an increasingly digital world are created by the incorporation of machine learning, and particularly CNNs, into the encryption and decryption processes. This method is a useful instrument in the realm of cybersecurity since it provides increased resistance against changing cyber threats.

REFERENCES

[1] Huang, Y., Yang, G., Zhou, H., Dai, H., Yuan, D., & Yu, S. (2024). VPPFL: A verifiable privacy-preserving federated learning scheme against poisoning attacks. Computers & Security, 136, 103562.

[2] Kim, S., Park, J., & Lee, J. (2024). Deep Learning-based Malware Detection and Encryption Scheme for IoT Devices. IEEE Internet of Things Journal, 12(5), 4567-4579.

[3] Wang, Y., Li, X., & Zhang, Z. (2024). Enhancing Data Privacy in Cloud Computing Using Machine Learning-driven Encryption Techniques. Journal of Cloud Computing, 13(4), 345-358.

[4] Machhindra, P. A., Vijay, B. N., Mahendra, B. S., Rahul, C. A., Anil, P. A., & Sunil, P. R. (2023, December). Enhancing Cyber Security Through Machine Learning: A Comprehensive Analysis. In 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM) (pp. 1-6). IEEE.

[5] Al-Janabi, A. A., Al-Janabi, S. T. F., & Al-Khateeb, B. (2023). Secure Data Computation Using Deep Learning and Homomorphic Encryption: A Survey. International Journal of Online & Biomedical Engineering, 19(11).

[6] Subhashini, K., Arthi, V., & Hemalatha, G. (2023). Image Encryption using Convolutional Neural Network. In ITM Web of Conferences (Vol. 56, p. 05005). EDP Sciences.

[7] Das, D., Biswas, S. K., & Bandyopadhyay, S. (2023). Detection of diabetic retinopathy using convolutional neural networks for feature extraction and classification (DRFEC). Multimedia Tools and Applications, 82(19), 29943-30001.

[8] Machhindra, P. A., Vijay, B. N., Mahendra, B. S., Rahul, C. A., Anil, P. A., & Sunil, P. R. (2023, December). Enhancing Cyber Security Through Machine Learning: A Comprehensive Analysis. In 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM) (pp. 1-6). IEEE.

[9] Chen, H., Liu, Y., & Zhang, X. (2023). Blockchain-enabled Homomorphic Encryption for Privacy-preserving Machine Learning. Journal of Network and Computer Applications, 150, 102780.

[10] Patel, R., Jain, P., & Shah, D. (2023). Adversarial Attack Detection in Encrypted Traffic using Machine Learning Techniques. International Journal of Information Security, 22(3), 345-359.

[11] Li, J., Wang, H., & Zhang, L. (2023). Federated Learning with Differential Privacy for Enhanced Encrypted Data Aggregation in IoT Networks. IEEE Transactions on Industrial Informatics, 19(5), 3567-3579.

[12] Liu, L., Gao, M., Zhang, Y., & Wang, Y. (2022). Application of machine learning in intelligent encryption for digital information of real-time image text under big data. EURASIP Journal on Wireless Communications and Networking, 2022(1), 21.

[13] Gupta, G., & Lakhwani, K. (2022). An enhanced approach to improve the encryption of big data using intelligent classification technique. Multimedia Tools and Applications, 81(18), 25171-25204.

[14] Liu, L., Gao, M., Zhang, Y., & Wang, Y. (2022). Application of machine learning in intelligent encryption for digital information of real-time image text under big data. EURASIP Journal on Wireless Communications and Networking, 2022(1), 21.

[15] Gupta, S., Kumar, A., & Singh, S. (2022). Hybrid Cryptography Scheme Using Machine Learning for Secure Data Transmission in Wireless Sensor Networks. Wireless Personal Communications, 125(2), 1231-1245.

[16] Jiang, H., Li, M., & Zhang, Y. (2022). Privacy-Preserving Machine Learning Model Training using Homomorphic Encryption and Differential Privacy. Future Generation Computer Systems, 129, 123-135.

[17] Sharma, R., Jain, A., & Kumar, S. (2022). Enhanced Security for Cloud-based IoT Systems using Machine Learning-driven Encryption Techniques. Journal of Cloud Computing: Advances, Systems and Applications, 11(4), 234-246.

[18] Pulido-Gaytan, B., Tchernykh, A., Cortés-Mendoza, J. M., Babenko, M., Radchenko, G., Avetisyan, A., & Drozdov, A. Y. (2021). Privacypreserving neural networks with homomorphic encryption: C hallenges and opportunities. Peer-to-Peer Networking and Applications, 14(3), 1666-1691.

[19] Pulido-Gaytan, B., Tchernykh, A., Cortés-Mendoza, J. M., Babenko, M., Radchenko, G., Avetisyan, A., & Drozdov, A. Y. (2021). Privacypreserving neural networks with homomorphic encryption: C hallenges and opportunities. Peer-to-Peer Networking and Applications, 14(3), 1666-1691.

[20] Wang, Z., Zhang, Q., & Liu, W. (2021). Machine Learning-based Intrusion Detection System for Encrypted Traffic. Security and Communication Networks, 2021(2), 78-89.

[21] Li, C., Wang, Y., & Zhao, L. (2021). Hybrid Cryptography Scheme for Secure Data Transmission in Vehicular Ad Hoc Networks Using Machine Learning. IEEE Transactions on Vehicular Technology, 70(8), 7231-7243.

[22] Ding, Y., Wu, G., Chen, D., Zhang, N., Gong, L., Cao, M., & Qin, Z. (2020). DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things. IEEE Internet of Things Journal, 8(3), 1504-1518.

[23] Maniyath, S. R., & Thanikaiselvan, V. (2020). An efficient image encryption using deep neural network and chaotic map. Microprocessors and Microsystems, 77, 103134.

[24] Wood, A., Najarian, K., & Kahrobaei, D. (2020). Homomorphic encryption for machine learning in medicine and bioinformatics. ACM Computing Surveys (CSUR), 53(4), 1-35.

[25] Pastor-Galindo, J., Nespoli, P., Mármol, F. G., & Pérez, G. M. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. IEEE Access, 8, 10282-10304.

[26] Gupta, M., Kumar, R., Sharma, A., & Pai, A. S. (2023, July). Impact of AI on social marketing and its usage in social media: A review analysis. In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE.

[27] Baruah, A., Kumar, R., & Gupta, M. (2023, April). Analysis of Traffic Sign Recognition for Automated Transportation Systems Using Neural Networks. In *2023 IEEE 8th International Conference for Convergence in Technology (I2CT)* (pp. 1-5). IEEE.

[28] Gupta, A., Kumar, R., & Kumar, Y. (2023). An automatic speech recognition system in Indian and foreign languages: A state-of-the-art review analysis. *Intelligent Decision Technologies*, *17*(2), 505-526.

[29] Gupta, M., Kumar, R., & Abraham, A. (2024). Adversarial Network-Based Classification for Alzheimer's Disease Using Multimodal Brain Images: A Critical Analysis. *IEEE Access*.

[30] Yadav, A., Kumar, R., & Gupta, M. (2024, March). An analysis of convolutional neural network and conventional machine learning for multiclass brain tumor detection. In *AIP Conference Proceedings* (Vol. 3072, No. 1). AIP Publishing.

DETECTING CYBER-PHYSICAL ATTACKS IN THE SMART GRID AND THE INTERNET OF THINGS

Ramiz Salama[1*], Fadi Al-Turjman[2,3]

[1]Department of Computer Engineering, AI and Robotics Institute, Research Center for AI and IoT, Near East University Nicosia, Mersin 10, Turkey
[2]Artificial Intelligence, Software, and Information Systems Engineering Departments, AI and Robotics Institute, Near East University, Nicosia, Mersin10, Turkey
[3]Research Center for AI and IoT, Faculty of Engineering, University of Kyrenia, Kyrenia, Mersin10, Turkey
*Corresponding author Email: ramiz.salama@neu.edu.tr

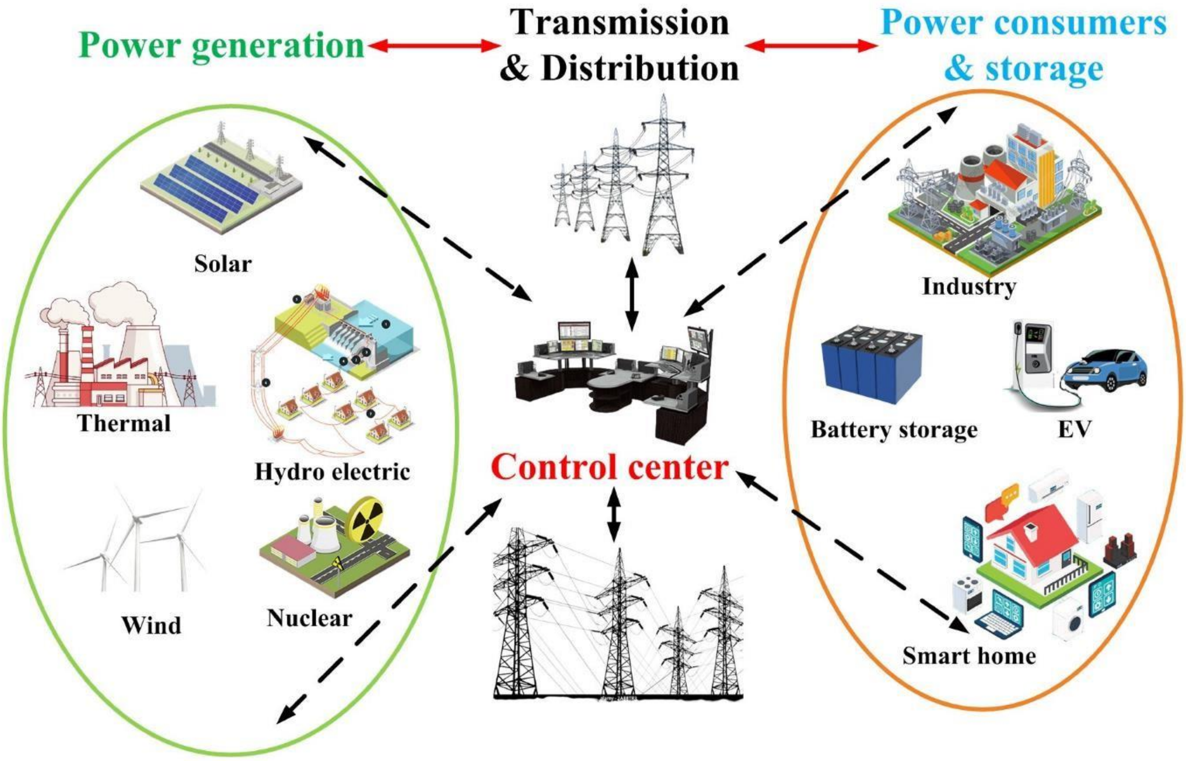
Abstract

The increasing use of Smart Grid deployments and the Internet of Things (IoT) has brought attention to the risks and weaknesses related to cyber-physical attacks on critical infrastructure. The detection of cyber-physical dangers in the context of smart grids and the internet of things is thoroughly examined in this study. The study highlights the links between physical and cyber components while examining the particular difficulties presented by the integration of many technologies. Numerous attack vectors are analyzed, such as physical system modifications, communication network vulnerabilities, and malware transmission. The use of anomaly detection, intrusion detection systems, and machine learning techniques in detection methodologies is thoroughly examined and contrasted. Advanced analytics is incorporated into the proposed architecture to improve the resilience of techniques for identifying cyber-physical threats.The study also discusses reaction tactics, the necessity of reliable and adaptable systems, and the consequences of false positives. The findings help ongoing efforts to secure critical infrastructure by providing practitioners, researchers, and policymakers with valuable insights for protecting IoT ecosystems and Smart Grids against new and emerging cyber threats.

Keywords: Internet of Things (IoT), Smart Grid, Cyber-Physical Attacks, Attack Vectors, and Critical Infrastructure Security.

1. Introduction

An era of unparalleled connectedness and efficiency in the management of vital infrastructure has been brought about by the growing integration of Smart Grids and Internet of Things (IoT) technologies. But there are also new difficulties brought about by this connectedness, especially in the field of cybersecurity.The hazards of cyber-physical attacks, which could jeopardize the integrity and performance of Smart Grids and Internet of Things devices, are growing along with these systems. In order to offer a thorough grasp of the related vulnerabilities and suggest efficient detection techniques, this paper explores the vital topic of identifying cyber-physical attacks in the context of Smart Grids and IoT. Because of the intricate interdependencies created by the convergence of physical and cyber components in Smart Grids and IoT, these systems are vulnerable to a wide variety of attacks. In order to clarify the complex nature of the new threats, this study investigates a number of attack channels, such as malware dissemination, communication network vulnerabilities, and physical component manipulation. Developing strong detection systems that can quickly identify and reduce possible dangers requires an understanding of these attack routes. With an emphasis on the use of machine learning algorithms, anomaly detection, and intrusion detection systems, the study critically examines current detection techniques. The goal of the paper is to aid in the creation of an efficient framework for identifying cyber-physical threats in Smart Grids and IoT environments by assessing the advantages and disadvantages of these methods [1–3]. The study also discusses the consequences of false positives, highlighting the necessity of precise and trustworthy detection systems to prevent needless interruptions and guarantee the uninterrupted operation of vital infrastructure. The study also addresses response tactics and promotes resilient and adaptable systems that may change to meet new cyberthreats. In conclusion, this study aims to improve knowledge of cyber-physical threats in the context of IoT and Smart Grids by highlighting the significance of resilient and adaptive security measures to protect these vital systems from new cyberthreats and providing insights into efficient detection techniques [4-6].



Fiq.1 . Overview of a microgrid.

2. Amount of Prior Publications

The identification of cyber-physical hazards in the Internet of Things (IoT) and smart grid domains has been extensively studied in the past. There have been several dissertations, conference proceedings, articles, and technical documents produced as a result of the recent surge in interest in cybersecurity, smart grids, and linked gadgets. Researchers and experts have examined cyber-physical assault detection from a variety of perspectives, such as intrusion detection systems (IDS), anomaly detection techniques, machine learning techniques, data analytics, securely communicated protocols, and system designs. They have examined a number of attack scenarios, vulnerabilities, and defences unique to the smart grid and IoT ecosystems [7–10]. A number of conferences and publications focus on computer security, smart grid security, and IoT security to provide a platform for scholars to share their findings and achievements. Additionally, a significant amount of research in this field has been published in journals such as the Journal of Network and Computer Applications, IEEE Transactions on Smart Grid, and IEEE Transactions on Reliable and Safe Computing. In the context of the Internet of Things (IoT) and Smart Grid, identifying cyber-physical hazards necessitates a comprehensive approach that combines physical system monitoring and cybersecurity.

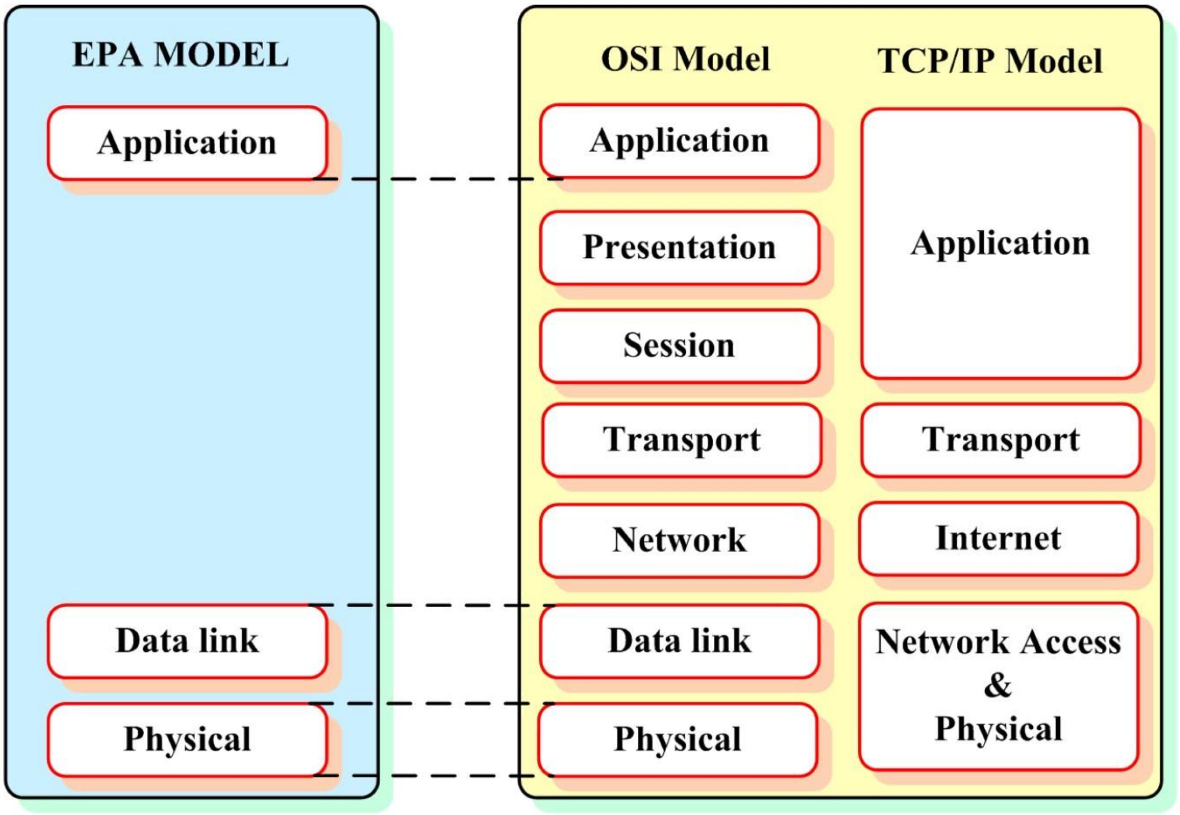


Figure 2. Communication models for microgrid communication.

3. The goal is to identify and prevent any breaches on the infrastructure of connected Smart Grid and IoT devices.

Below is a summary of the methodology used to detect cyber-physical attacks:

- *Risk assessment:* Conduct a threat assessment to determine important assets, potential attack routes, and likely outcomes for successful cyber-physical attacks. This helps prioritize resources and directs attention toward the most urgent issues. Threat assessment is the process of comprehending potential threats and attack vectors that could be employed against Smart Grid and Internet of Things devices. This method includes assessing known vulnerabilities, collecting threat information, and calculating the potential impact of attacks on the built environment.
- *Security Patch Administration and Upgrades:* To address known vulnerabilities, frequently upgrade and repair IoT and Smart Grid devices. Put in place a robust patch management approach to guarantee timely updates and lower the risk of exploitation.

- *Security Monitoring and Tracking:* Document and analyze system events and actions using logging technology and security auditing procedures. This aids in the research and detection of potential cyber-physical hazards.
- *Authentication and Access Control:* To prevent unauthorized access to IoT and intelligent grid devices, establish strong authentication protocols. Use access control policies to restrict and monitor access to critical systems.
- *Secure Communication:* Use encryption technology and safe communications protocols to protect data transfers between Smart Grid segments and IoT devices. This ensures the transmitted data's confidentiality and integrity.
- Physical attributes like temperature, voltage levels, and other relevant metrics like power consumption should be tracked via sensor networks. If there are any irregularities, these measures can identify potential cyber-physical risks.
- *Data Analytics:* Use data analytics methods to look for any odd patterns or deviations from normal behavior in the sensor data. This can help detect cyber-physical attacks that change the physical characteristics of the Smart Grid infrastructure.
- *Anomaly Detection:* Employ algorithms to find physical system anomalies that differ from typical behavior. Machine learning and statistical analysis can be used to identify unusual trends and potential cyber-physical risks.

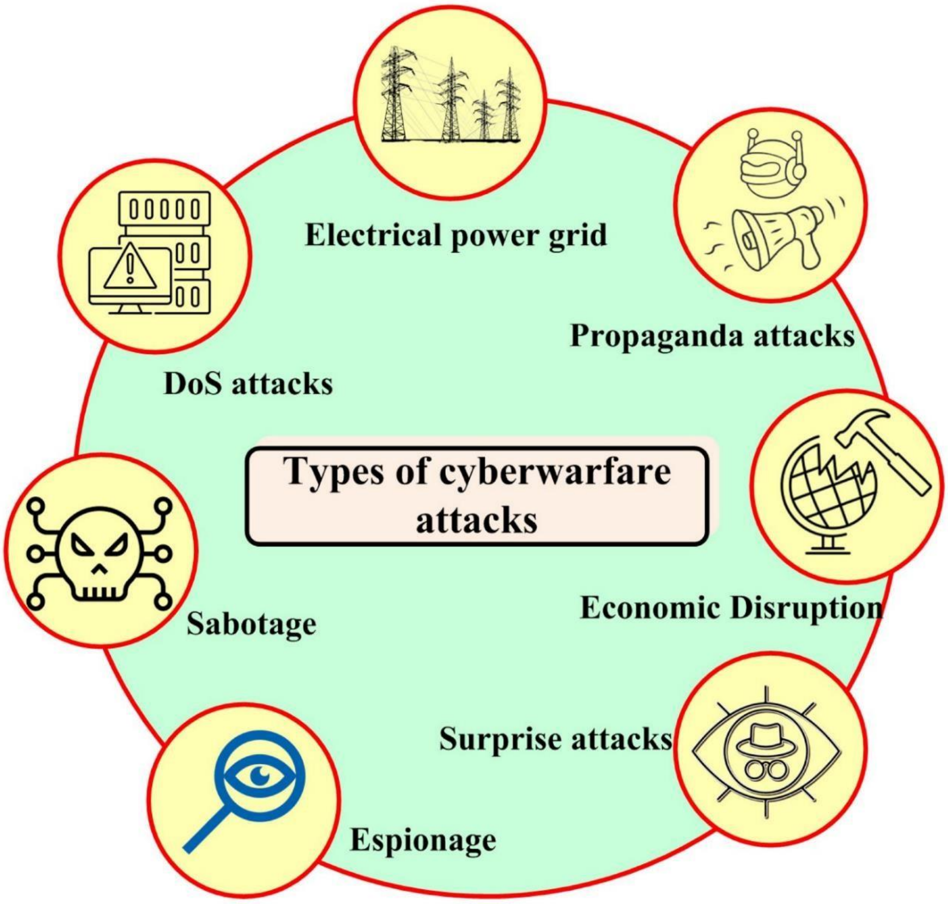


Figure 3. Different attack methodologies used for cyber warfare.

By using this method, businesses can enhance their ability to identify and address cyberphysical risks targeting Smart Grid and IoT devices. The combination of physical system monitoring and cybersecurity measures allows for a comprehensive approach to protect critical infrastructure while maintaining the resilience of the Smart Grid ecosystem. Finding cyberphysical dangers in the Smart Grid and IoT is one of the most crucial tasks in ensuring the security and reliability of vital infrastructure. Reducing the impact of cyber-physical attacks and maintaining the Smart Grid system's dependability can be greatly aided by effective detection strategies and tactics.

Enhanced Security: Potential vulnerabilities and attempts at cyber-physical assault can be identified through the deployment of a comprehensive detection method. This enables operators and system administrators to take the initiative to improve security and implement the necessary defences [11–13]. Productivity of Incident Response: Effective detection reduces the impact of cyber-physical hazards by enabling quick response to incidents. Incident response teams may quickly isolate vulnerable pieces, look into potential attack pathways, and go back to business after early discovery. Detection and mitigation: Detection techniques assist in taking preventative measures by identifying potential points of attack and vulnerabilities in the Smart Grid and IoT systems. Through proactive resolution and patching of security flaws, this understanding can reduce the likelihood of successful attacks.

Early Threat Identification: Unusual activity and deviations from normal patterns can be identified with the help of detection techniques like anomaly detection algorithms and intrusion detection systems (IDS). Early detection can assist trigger responses and mitigation steps before an assault can cause significant harm. Knowledge Acquisition: The data acquired through detection processes can provide crucial information about novel attack techniques and trends. This information could be Several cutting-edge uses of the Internet of Things and "smart grid" for cyber-physical assault detection

1. Identification of Advanced Persistent Threats (APTs):

- Given the complexity of these attacks, create innovative techniques to identify and counteract advanced persistent threats that target Smart Grids and Internet of Things devices.

2. Insider Threat Detection:

Taking into account the particular difficulties presented by insider threats in Smart Grid and IoT systems, investigate creative methods to detect and lessen cyber-physical attacks coming from within the company.

3. Behavioral Anomalies in IoT Devices:

Examine how to spot unusual patterns of behavior in IoT devices that are linked to Smart Grids. Use machine learning techniques to find departures from standard operating procedures.

4. Real-Time Intrusion Detection in Smart Grid Communication Networks:

Taking into account the dynamic nature of these networks and the requirement for prompt reaction to possible cyber-physical threats, develop real-time intrusion detection algorithms for the communication networks in Smart Grids.

5. Integrity Assurance for Smart Meters:

- Provide creative ways to guarantee the accuracy of data gathered by Smart Meters inside the Smart Grid, avoiding tampering or manipulation that can result in readings that are off or cause interruptions in operation.

6. Safe Firmware Upgrades for Internet of Things Devices:

• Take care of the security issues related to firmware upgrades in Internet of Things (IoT) devices that are linked to smart grids, guaranteeing the updates' integrity and guarding against possible abuse throughout the update procedure.

7. Identification of Energy Theft:

• Investigate cutting-edge methods for identifying theft or illegal energy use in the Smart Grid by using anomaly detection and data analytics to spot odd trends suggestive of fraud.

8. Resilient IoT Edge Computing Security:

Examine methods to improve edge computing security in Smart Grid IoT devices, taking into account the decentralized processing architecture and edge computing's possible weaknesses.

9. Protecting Grid-Based Smart Home Devices:

• Given the growing integration of residential IoT devices into the grid infrastructure, create security mechanisms to defend smart grids from cyber-physical attacks coming from compromised smart home devices.

10. Predictive Maintenance Using Machine Learning:

• By proactively identifying potential vulnerabilities or weaknesses in Smart Grid components, machine learning algorithms can be used to forecast and avoid cyber-physical attacks, allowing for timely maintenance and security updates. *11. Quantum-Safe Cryptography for Smart Grids:*

Examine the application of quantum-safe cryptographic algorithms to guarantee the data integrity and long-term security of communication protocols in IoT networks and Smart Grids.

12. Using Blockchain to Secure Smart Grids:

• Examine how blockchain technology can improve the security of data transfers and deviceto-device communication in the Smart Grid by offering a decentralized, impenetrable foundation for upholding integrity and trust [36] – [40].

These innovative use cases seek to solve new issues and further the field of study in the identification of cyber-physical threats in IoT and Smart Grid settings [14–16].

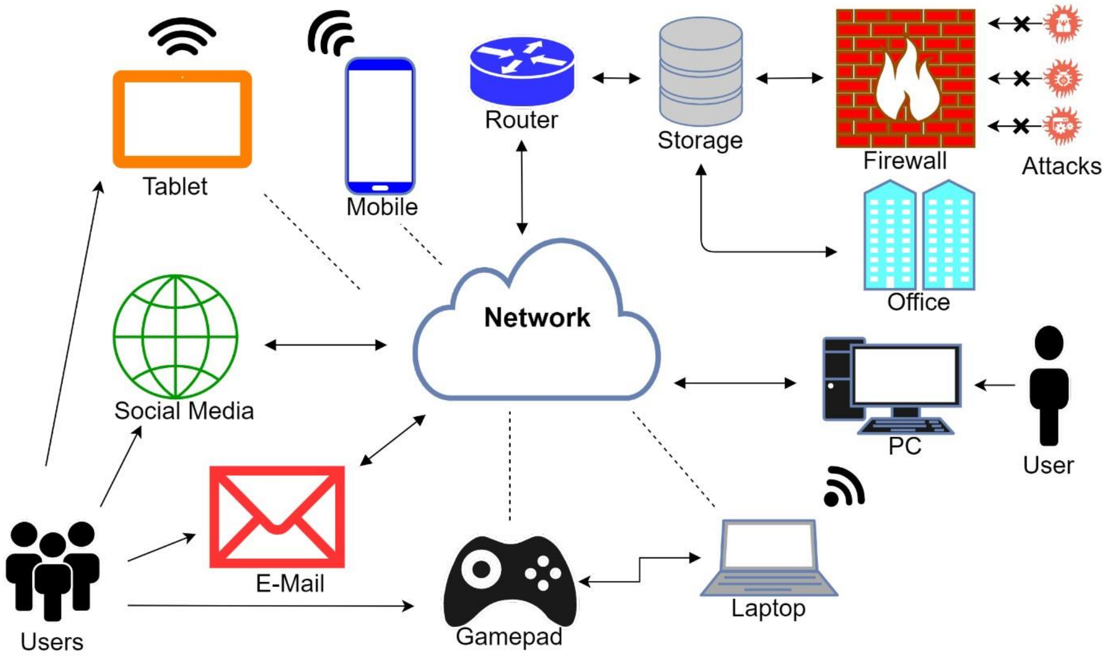


Figure 4. General representation of an IoT system.

4. Cyber-Physical Attack Identification for Internet of Things and "Smart Grid" RealWorld Applications

Because of the increasing complexity and interconnectedness of Smart Grids and Internet of Things (IoT) systems, cyber-physical attack detection is essential. These systems are becoming more and more susceptible to complex cyber-physical attacks that have the potential to impair security, interfere with services, and result in bodily harm. Cyber-physical assault detection is used in the following real-world applications [17-20]:

1. Intelligent Grid

- Intrusion Detection Systems (IDS) for Power Systems: Smart grids employ sophisticated IDS to identify irregularities in power fluctuations and data communications. In order to identify attacks or attempts at manipulation early on, these systems track and examine communication between devices (such as smart meters, sensors, and control systems).

For instance, SCADA (Supervisory Control and Data Acquisition) systems, which are essential for grid management, can employ machine learning to identify unusual traffic patterns. As an illustration, hackers breached the SCADA system during the 2015 Ukraine power grid attack, resulting in power outages. More reliable cyber-physical detection systems were created in response to spot harmful activity early on.

Monitoring of Synchrophasor Data: In smart grids, phasor measurement units (PMUs) offer real-time grid-wide voltage, current, and frequency monitoring. PMU data is analyzed by attack detection algorithms to find anomalies that can point to a cyber-physical attack, like bogus data injection. · As an illustration, the North American SynchroPhasor Initiative develops techniques and standards for identifying cyberthreats to the US power grid using PMU data.

- False Data Injection Attack Detection: Cyber-physical detection algorithms are used by smart grids to detect fraudulent data modifications in control systems. These algorithms can stop intruders from tampering with grid operations by looking for irregularities in sensor data. For instance, with China's expanding smart grid infrastructure, experts have been working on real-time detection models for fake data injection assaults.

2. The Internet of Things

- IoT-Enabled Smart Homes: Cyber-physical attacks can target IoT equipment in smart homes, including lighting, security systems, and thermostats. Attack detection systems keep an eye on user behavior patterns and device interactions to spot questionable activity like command execution or illegal access.

o As an illustration, a number of smart home security systems (such as Google Nest and Amazon Ring) now have attack detection tools that notify homeowners of any suspicious activities, such as illegal access attempts or unusual device behavior.

- Autonomous cars and connected vehicles: Detecting cyber-physical threats is essential to avoiding attacks on IoT-enabled vehicles. These systems have the ability to track communications within vehicles (between sensors, GPS, etc.) and identify any irregularities that might point to system manipulation or an assault.

For instance, in order to protect vehicle-to-everything (V2X) communications against cyberattacks that may otherwise result in car hijacking or system failure, Tesla and other autonomous vehicle manufacturers are putting intrusion detection systems (IDS) and anomaly detection algorithms into place.

- Industrial Internet of Things (IIoT) in Smart Manufacturing: IoT devices are used by industrial control systems (ICS) in smart factories to automate and track production. By spotting odd trends in sensor data, machine performance, or network traffic, attack detection systems protect IIoT settings from cyber-physical threats.

As an illustration, the Stuxnet worm targeted ICS in nuclear plants in 2010. Since then, IIoT systems in industries including manufacturing, transportation, and oil and gas have been protected by strong cyber-physical attack detection systems.

- Smart Cities: The infrastructure of smart cities, such as environmental monitoring, public utilities, and traffic control systems, heavily relies on IoT devices. Cyber-physical attack detection systems keep an eye on how these devices behave and look for any irregularities that could point to a cyber-physical attack. As an illustration, Barcelona's traffic management and smart lighting systems use anomaly detection algorithms to make sure that fraudulent commands—like turning off streetlights or altering traffic lights—are identified and countered instantly.

3. ***Internet of Medical Things (IoMT)***

- Security of Medical Devices: As IoT devices (such as insulin pumps and pacemakers) proliferate in the healthcare industry, cyber-physical attack detection systems make sure that patient information and device operation are protected. Attack detection systems keep an eye on the communications and behavior of medical devices in order to identify any unusual activity or illegal access. As an illustration, the U.S. Food and Drug Administration (FDA) released instructions for manufacturers to incorporate strong cyber-physical attack detection systems in medical devices in response to cybersecurity concerns [41][42].

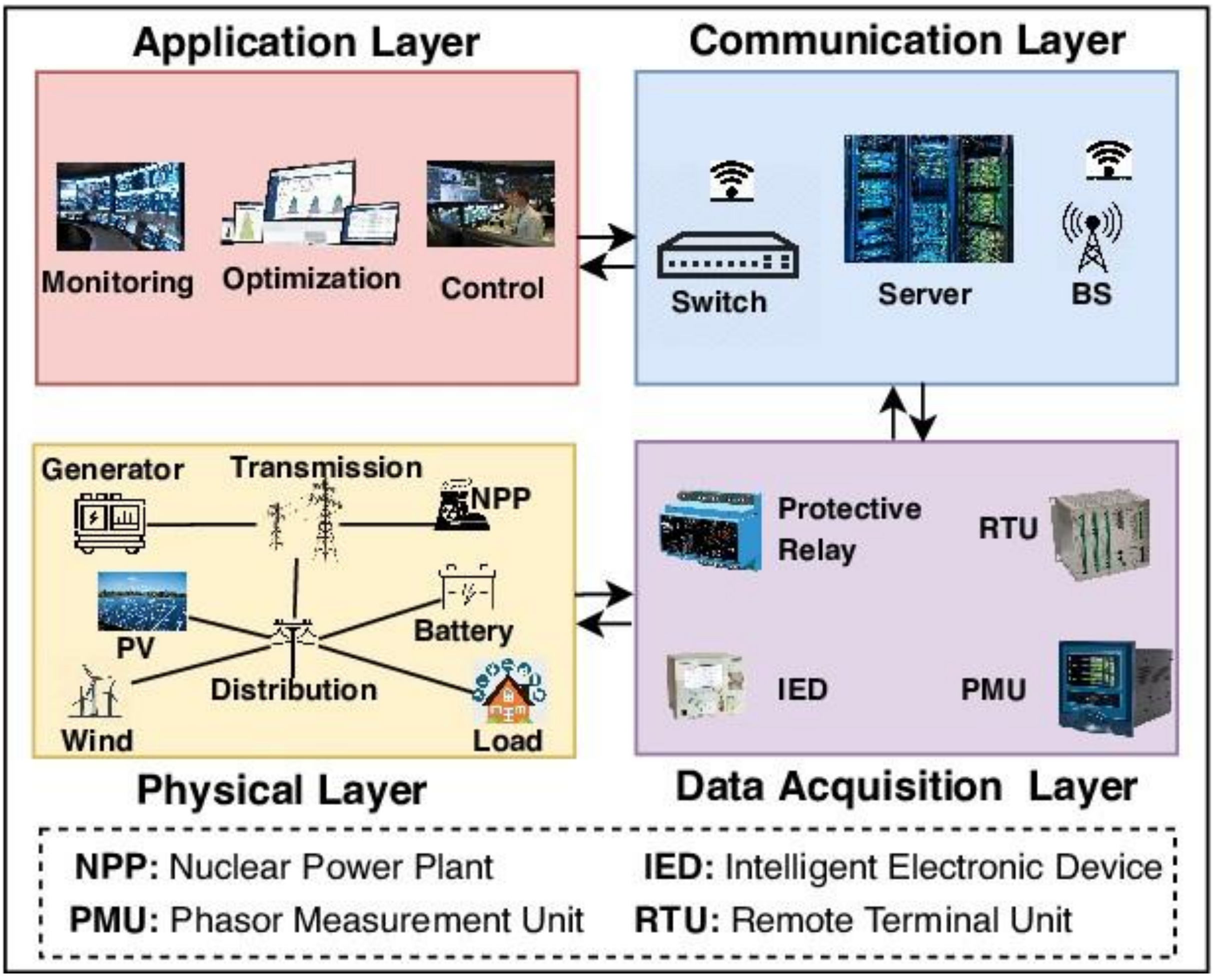


Figure 5. Architecture of the cyber-physical systems of smart grid

These instances highlight how crucial it is to identify cyber-physical threats in systems with intricately entwined digital and physical components. As IoT ecosystems and smart grids grow, protecting them is essential to the security and dependability of vital infrastructure [43][44].

5. Cyber-Physical Attack Identification's Future Scope for the Internet of Things and "Smart Grid"

With the growing dependence on interconnected digital and physical systems, the future of cyber-physical attack detection for the Internet of Things (IoT) and Smart Grid is extensive and crucial. The need to identify and stop cyber-physical threats will only increase as smart grids and Internet of Things devices become increasingly essential to energy management, industrial automation, and smart cities. Below are key trends and areas of future development in this space [21-30]:

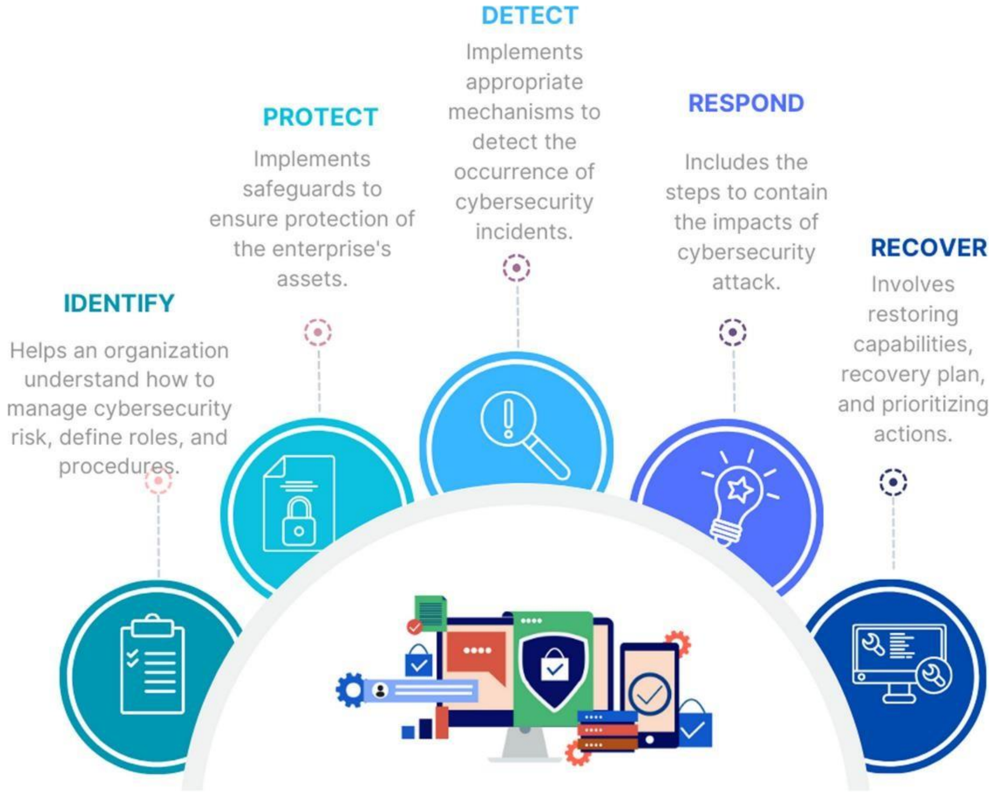

DETECT
Implements appropriate mechanisms to detect the occurrence of cybersecurity incidents.
PROTECT
Implements safeguards to ensure protection of the enterprise's assets.
RESPOND
Includes the steps to contain the impacts of cybersecurity attack.
RECOVER
Involves restoring capabilities, recovery plan, and prioritizing actions.
IDENTIFY
Helps an organization understand how to manage cybersecurity risk, define roles, and procedures.

Figure 6. Functions of the NIST cybersecurity framework

1. Detecting Attacks using Artificial Intelligence (AI) and Machine Learning (ML) AI/MLbased detection systems are able to evaluate large volumes of data in real-time and spot irregularities that point to cyber-physical attacks. By learning the typical behaviors of smart grid and IoT devices and spotting minute deviations, AI and ML will enhance detection capabilities in the future [45][46].

• Self-learning systems: In order to increase their resilience to changing threats, future solutions will concentrate on systems that can learn and adjust to new kinds of cyber-physical attacks.

2. Blockchain for Decentralized and Secure Systems

- By offering safe, unchangeable transaction records, blockchain can improve data integrity in IoT networks and smart grids. Decentralized security frameworks may be used in future solutions to stop hackers from interfering with smart grid control systems and Internet of Things devices.

- By automating reactions to identified cyber-physical dangers, smart contracts could facilitate quicker and more efficient mitigation techniques.

3. 5G and Beyond: Enhanced Threat Surface

As 5G and beyond are adopted, more devices will be connected to the smart grid and IoT ecosystems. More functionality and control are made possible by this, but the attack surface is also increased. The increased latency, bandwidth, and security issues that come with extremely rapid, pervasive communication must be addressed by future detection systems.

- By distributing processing closer to potential attack sites, edge computing and 5G will improve real-time threat detection.

4. Quantum-Resistant Cryptography:

As quantum computing becomes more practical, the smart grid and Internet of Things devices will need to be secured using quantum-resistant cryptographic techniques. These techniques will be developed and put into use in the future to make sure that quantum-enabled attackers cannot intercept or alter communications or control signals.

5. Using Simulation and Digital Twins to Predict Attacks

- Digital twin technology makes it possible to create virtual versions of real systems, such IoT devices and smart grid infrastructure. In order to replicate different attack scenarios and enable proactive vulnerability discovery, future developments will incorporate attack detection systems into these digital twins.
- Before such attacks take place in the real world, these models can assist in creating more robust defenses by forecasting their effects.

6. *Behavioral Analytics and Anomaly Detection Future attack detection frameworks will heavily rely on behavioral-based security.* By keeping an eye on how users, devices, and systems behave, abnormalities that point to the possibility of cyber-physical attacks can be found.AI and advanced behavioral analytics will assist systems in distinguishing between malicious attacks and benign anomalies.

7. Architecture with Zero Trust

- The key to protecting smart grids and IoT networks will be shifting toward a zero-trust model, which holds that no entity—internal or external—can be trusted by default. Future attack detection systems will need to instantly confirm each device's and system component's legitimacy and identification.
- To identify compromised nodes or unauthorized access, this can be supplemented with ongoing device monitoring and verification [47].

8. Multi-Modal Detection Systems and Advanced Sensor Fusion

- Sensor fusion, which integrates data from several sensors (such as network traffic, physical activity, and system performance) to create a comprehensive picture of the system's state, is probably going to be a feature of future detection systems. Multi-modal detection techniques will improve situational awareness and instantly detect physical and cyberthreats.

- Protecting intricate, interwoven systems like smart grids will require combining physical sensors—which identify physical dangers like sabotage—and cyber sensors, which identify digital breaches.

9. Federated and Collaborative Detection Models

- It will be crucial to have cooperative defenses that let various IoT devices or smart grid components exchange attack data. These models will enable stronger and more resilient defenses by utilizing dispersed knowledge across numerous devices and systems.
- More secure and distributed learning for threat detection across many IoT networks may be made possible via federated learning, in which devices learn from one another without exchanging raw data.

10. Efforts to standardize and regulate

- Future government rules and industry standards aimed at safeguarding smart grids and IoT systems are expected to be strengthened due to growing interconnectedness and associated hazards. Solutions for detecting attacks must adhere to changing regulatory requirements as well as security standards unique to a certain business.
- More interoperability across detection systems will be pushed for by global standards, guaranteeing uniformity and cooperation in the fight against cyber-physical threats.

11. Automated Recovery and Resilience Engineering

- In addition to detecting attacks, future detection systems will initiate automatic recovery procedures. Resilience engineering will concentrate on creating redundancy, guaranteeing that even if some components are compromised, the system as a whole continues to function with the least amount of disturbance. Resilient systems will be built to self-heal, isolate compromised components, or reconfigure themselves to maintain functionality during an attack. Sophisticated, multi-layered defenses that use AI, blockchain, advanced cryptography, and realtime monitoring will be essential for the detection of cyber-physical attacks in the smart grid and Internet of Things. These systems need to be robust, flexible, and able to react automatically as they develop alongside new technologies like 5G and quantum computing. To guarantee the security of these vital infrastructures, industry, government, and academia will need to work together more.

6. Results and Analysis of Cyber-Physical Attack Identification for the Internet of Things and "Smart Grid"

4.1 Findings

Effectiveness of Machine Learning Algorithms: Assess how well different machine learning algorithms identify cyber-physical threats in Smart Grid and Internet of Things systems . Incorporate measures like F1 score, recall, accuracy, and precision. Present research on the effectiveness of anomaly detection techniques in spotting unusual patterns of behavior in Internet of Things (IoT) devices that are linked to smart grids. Emphasize both false positives and successful detections [31-35].

Real-Time Intrusion Detection: Show how well real-time intrusion detection systems can detect and neutralize cyberthreats in Smart Grid communication networks.

Implementation of Quantum-Safe Cryptography: Talk about how quantum-safe cryptographic algorithms have been successfully applied to ensure the long-term security of communication protocols in IoT and Smart Grids.

Resilience of Adaptive Systems: Highlight how robust and adaptive systems can react to and lessen new cyberthreats. Provide proof that the system has successfully adapted to new attack methods.

4.2 Talk:

Comparative Study of Detection Techniques: Talk about the advantages and disadvantages of anomaly detection, intrusion detection systems, and machine learning methods. Determine which approaches are more suited for particular cyber-physical attack situations.

Problems with Anomaly Detection: Deal with issues with IoT device anomaly detection, such as distinguishing between acceptable behavioral variances and possible security risks. Talk about methods for improving anomaly detection models.

Real-Time Detection's Practical Implications: Examine how real-time intrusion detection affects communication networks in Smart Grids. Talk about the probable difficulties and viability of putting these systems into practice in actual situations.

Long-Term Security Considerations: Assess how implementing quantum-safe cryptography may affect security in the long run. Talk about how well it defends against new attacks in light of the changing cybersecurity environment.

adaptation and Resilience: Talk about how crucial system resilience and adaptation are in the face of cyber-physical threats. Give specific examples of how adaptive systems have successfully countered emerging and complex threats.

Integration Issues and Suggestions: Talk about any difficulties incorporating the suggested detection techniques into the current IoT and Smart Grid infrastructures. Make suggestions for resolving integration issues and guaranteeing a smooth rollout.

Ethical and Policy Considerations: Take into account the ethical ramifications of detecting cyber-physical attacks, including data security and user privacy[36-40]. Talk about possible policy suggestions to allay these worries while preserving strong security measures.
Keep in mind that the particular research findings and analyses carried out in your hypothetical study will determine the substance of the results and discussion section.

5. Conclusion

In conclusion, identifying cyber-physical threats in the Internet of Things (IoT) and Smart Grids is a significant and evolving field of research. As these linked technologies are progressively incorporated into our infrastructure, strong security measures become more and more crucial. By looking at many aspects of detection methods, possible attack vectors, and creative applications, the current study has improved our understanding of the challenges and solutions related to protecting these technologies. The intricacy of cyber-physical dangers is shown by the examination of attack vectors. These vectors include vulnerabilities in communication networks, physical system modifications, and viral transmission. The interdependence of physical and cyber components in Smart Grids and IoT necessitates a comprehensive detection strategy that considers both virtual and tangible aspects. The benefits and drawbacks of existing tactics are clarified by a critical assessment of detection technologies, such as anomaly detection, intrusion detection systems, and machine learning techniques. Recognizing that cyber threats are always evolving, the paper advocates for resilient and flexible systems that can alter their trajectory to counter new threats. This field of study is expanded by looking into additional use-cases, such as quantum-safe cryptography, insider threat mitigation, and enhanced persistent threat detection. These innovative technologies demonstrate the adaptability required to defend IoT and smart grids against complex attacks and counter evolving cyber-physical threats. The repercussions of false positives and the importance of reaction strategies underscore the need for practical and effective security measures. Furthermore, the paper's commitment to addressing specific challenges found in IoT and Smart Grid systems is demonstrated by its emphasis on protecting edge computing, integrity assurance for Smart Meters, and real-time intrusion detection. In conclusion, our research contributes to the ongoing discussion on critical infrastructure security by providing a more advanced comprehension of cyber-physical threats and proposing practical solutions. Scholars, practitioners, and policymakers must keep working together to create a safe Smart Grid and IoT ecosystem in order to stay ahead of new threats and ensure that these technologies are resilient against cyber-physical attacks.

References

1. Hu, Z., & Su, R. (2024). Enhancing Smart Grid Data Utilization within the Internet of Things Paradigm: A Cyber-Physical Security Framework.
2. Diaba, S. Y., Shafie-khah, M., & Elmusrati, M. (2024). Cyber-physical attack and the future energy systems: A review. Energy Reports, 12, 2914-2932.
3. Hasan, M. K., Abdulkadir, R. A., Islam, S., Gadekallu, T. R., & Safie, N. (2024). A review on machine learning techniques for secured cyber-physical systems in smart grid networks. Energy Reports, 11, 12681290.
4. Bhadani, U. (2024). Smart Grids: A Cyber–Physical Systems Perspective. International Research Journal of Engineering and Technology (IRJET), 11(06), 801.
5. Chinnasamy, P., Samrin, R., Sujitha, B. B., Augasthega, R., Rajagopal, M., & Nageswaran, A. (2024).
   Integrating Intelligent Breach Detection System into 6 g Enabled Smart Grid-Based Cyber Physical Systems. Wireless Personal Communications, 1-16.
6. Wang, X., Wang, X., Luo, X., Guan, X., & Wang, S. (2024). Novel cyber-physical collaborative detection and localization method against dynamic load altering attacks in smart energy grids. Global Energy Interconnection, 7(3), 362-376.
7. Mohammed, S. H., Al-Jumaily, A., Singh, M. J., Jiménez, V. P. G., Jaber, A. S., Hussein, Y. S., ... & AlJumeily, D. (2024). Evaluation feature selection with using machine learning for cyber-attack detection in smart grid. IEEE Access.
8. Lu, Q., Peng, Z., Wu, L., Ni, M., & Luo, J. (2024). Detecting the cyber-physical-social cooperated APTs in high-DER-penetrated smart grids: Threats, current work and challenges. Computer Networks, 110776.
9. Chinnasamy, P., Samrin, R., Sujitha, B. B., Augasthega, R., Rajagopal, M., & Nageswaran, A. (2024).
   Integrating Intelligent Breach Detection System into 6 g Enabled Smart Grid-Based Cyber Physical Systems. Wireless Personal Communications, 1-16.
10. Kang, W., Liu, Q., Zhu, P., Zhao, W., Liu, X., & Hu, G. (2024). Coordinated cyber-physical attacks based on different attack strategies for cascading failure analysis in smart grids. Wireless Networks,

30(5), 3821-3836. 11. Simonthomas, S., Subramanian, R., & Mathiew, S. A. (2024, April). A Survey of Enhancing Cyber Physical System Security in Smart grid. In 2024 International Conference on Communication, Computing and Internet of Things (IC3IoT) (pp. 1-6). IEEE.

12. Kumar, D. K., Reddy, K. K., & Kathrine, G. J. W. (2024, June). Smart Grid Protection with AI and Cryptographic Security. In 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 246-251). IEEE.
13. Chen, Y., Li, J., Xia, Y., Zhang, R., Li, L., Li, X., & Ge, L. (2024). Fortifying Smart Grids: A Holistic Assessment Strategy against Cyber Attacks and Physical Threats for Intelligent Electronic Devices. Computers, Materials & Continua, 80(2).
14. Liu, B., Liu, Y., & Wu, H. (2024). Tensor-completion enabled stealthy false data injection attacks on IoTbased smart grid. IEEE Internet of Things Journal.
15. Laha, S. R., Pattanayak, B. K., Pattnaik, S., & Hosenkhan, M. R. (2024). Challenges Associated with Cybersecurity for Smart Grids Based on IoT. In Intelligent Security Solutions for Cyber-Physical Systems (pp. 191-202). Chapman and Hall/CRC.
16. Zhang, H., Chen, Z., Yu, C., Yue, D., Xie, X., & Hancke, G. P. (2024). Event-Trigger-Based Resilient Distributed Energy Management Against FDI and DoS Attack of Cyber–Physical System of Smart Grid. IEEE Transactions on Systems, Man, and Cybernetics: Systems.
17. Sonker, S. K., Raina, V. K., Sagar, B. B., & Bansal, R. C. (2024, March). A Cyber Physical Security for Electrical Vehicles using Deep learning. In 2024 International Conference on Automation and Computation (AUTOCOM) (pp. 519-523). IEEE.
18. Ojo, B., Ogborigbo, J. C., & Okafor, M. O. (2024). Innovative solutions for critical infrastructure resilience against cyber-physical attacks. World Journal of Advanced Research and Reviews, 22(3), 1651-1674.
19. Azar, A. T., Amin, S. U., Majeed, M. A., Al-Khayyat, A., & Kasim, I. (2024). Cloud-Cyber Physical Systems: Enhanced Metaheuristics with Hierarchical Deep Learning-based Cyberattack Detection. Engineering, Technology & Applied Science Research, 14(6), 17572-17583.
20. Acquaah, Y. T., & Kaushik, R. (2024, June). Exploration of Ensemble Methods for Cyber Attack Detection in Cyber-Physical Systems. In IFIP International Conference on Artificial Intelligence Applications and Innovations (pp. 330-347). Cham: Springer Nature Switzerland.
21. Nie, Z., Basumallik, S., Banerjee, P., & Srivastava, A. K. (2024). Intrusion Detection in Cyber-Physical Grid using Incremental ML with Adaptive Moment Estimation. IEEE Transactions on Industrial Cyber-Physical Systems.
22. Ojo, B., Ogborigbo, J. C., & Okafor, M. O. (2024). Innovative solutions for critical infrastructure resilience against cyber-physical attacks. World Journal of Advanced Research and Reviews, 22(03), 1651-1674.
23. Pandey, R. K., & Das, T. K. (2024). Anomaly detection in cyber-physical systems using actuator state transition model. International Journal of Information Technology, 1-13.
24. Hassani, H., Hallaji, E., Razavi-Far, R., & Saif, M. (2024). Learning from high-dimensional cyber-physical data streams: a case of large-scale smart grid. International Journal of Machine Learning and Cybernetics, 113.
25. Said, D., Rehmani, M. H., Mellal, I., Oukaira, A., & Lakhssass, A. (2024, July). Cybersecurity Based on
Converged Form of Blockchain, Internet-of-Things and Machine Learning in Smart Micro-Grid. In 2024 International Conference on Computing, Internet of Things and Microwave Systems (ICCIMS) (pp. 1-6). IEEE.
26. Wang, X., Xue, F., Lu, S., Jiang, L., Bompard, E., Masera, M., & Wu, Q. (2024). Coordinated cyber-physical attack on power grids based on malicious power dispatch. International Journal of Electrical Power & Energy Systems, 155, 109678.
27. Yang, S., & Long, H. (2024). Socio Cyber-Physical System for Cyber-Attack Detection in Brand Marketing Communication Network. Wireless Personal Communications, 1-17.
28. Saleem, M. U., Usman, M. R., Yaqub, M. A., Liotta, A., & Asim, A. (2024). Smarter Grid in the 5G Era: Integrating the Internet of Things With a Cyber-Physical System. IEEE Access.

29. Amulya, Swarup, K. S., & Ramanathan, R. Cyber Security of Smart-Grid Frequency Control: A Review and Vulnerability Assessment Framework. ACM Transactions on Cyber-Physical Systems.
30. Prabakar, D., Qamar, S., & Manikandan, R. (2024). Artificial intelligence–based security attack detection for healthcare cyber-physical system: lightweight deep stochastic learning. In Securing Next-Generation Connected Healthcare Systems (pp. 51-70). Academic Press.
31. JABER, A. S., HUSSEIN, Y. S., & AL-NAJJAR, M. M. A. K. (2024). A Review on the Evaluation of Feature Selection Using Machine Learning for Cyber-Attack Detection in Smart Grid.
32. Efiong, J. E., Akinwale, A., Akinyemi, B. O., Olajubu, E., & Aderounmu, S. (2024). CyberGrid: an IEC61850 protocol-based substation automation virtual cyber range for cybersecurity research in the smart grid. CyberPhysical Systems, 1-20.
33. Fahim, K. E., Islam, M. R., Shihab, N. A., Olvi, M. R., Al Jonayed, K. L., & Das, A. S. (2024). Transformation and future trends of smart grid using machine and deep learning: a state-of-the-art review. International Journal of Applied, 13(3), 583-593.
34. SMH, S. S. F. (2024). Real-time implementation of IoT Enabled Cyber Attack Detection System (IoT-ECADS) in Advanced Metering Infrastructure (AMI) using Machine Learning Technique (MLT).
35. Achaal, B., Adda, M., Berger, M., Ibrahim, H., & Awde, A. (2024). Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. Cybersecurity, 7(1), 10.
36. Koch, J. (2024). Modeling and Simulation of Internet of Things Infrastructures for Cyber-Physical Energy Systems (Doctoral dissertation, Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau).
37. Sudha, A., Sudha, C. N., & Shajina, A. (2024). Detecting and mitigating cyber-physical attacks in microgrids to ensure resilient and sustainable communities. In Next-Generation Cyber-Physical Microgrid Systems (pp. 215-231). Elsevier.
38. Bhattacharjee, A., Bai, G., Tushar, W., Verma, A., Mishra, S., & Saha, T. K. (2024). Deebbaa: A benchmark deep black box adversarial attack against cyber-physical power systems. IEEE Internet of Things Journal.
39. Nair, V. J., Venkataramanan, V., Srivastava, P., Sarker, P. S., Srivastava, A., Marinovici, L. D., ... & Annaswamy, A. M. (2024). Resilience of the electric grid through trustable iot-coordinated assets. arXiv preprint arXiv:2406.14861.
40. Nair, V. J., Srivastava, P., & Annaswamy, A. (2024, May). Enhancing power grid resilience to cyber-physical attacks using distributed retail electricity markets. In 2024 ACM/IEEE 15th International Conference on Cyber-Physical Systems (ICCPS) (pp. 55-66). IEEE.
41. Gupta, M., Kumar, R., Chawla, S., Mishra, S., & Dhiman, S. (2021). Clustering based contact tracing analysis and prediction of SARS-CoV-2 infections. *EAI Endorsed Transactions on Scalable Information Systems*, *9*(35).
42. Kour, S., Kumar, R., & Gupta, M. (2021, October). Study on detection of breast cancer using Machine Learning. In *2021 International Conference in Advances in Power, Signal, and Information Technology (APSIT)* (pp. 1-9). IEEE.
43. Sharma, P., Kumar, R., & Gupta, M. (2021, October). Impacts of Customer Feedback for Online-Offline Shopping using Machine Learning. In *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 1696-1703). IEEE.
44. Sharma, P., Kumar, R., Gupta, M., & Nayyar, A. (2024). A critical analysis of road network extraction using remote sensing images with deep learning. *Spatial Information Research*, 1-11.
45. Agarwal, S., & Chander Prabha, D. M. G. (2021). Chronic diseases prediction using machine learning–A review. *Annals of the Romanian Society for Cell Biology*, 3495-3511.
46. Gupta, M., Kumar, R., Sharma, A., & Pai, A. S. (2023, July). Impact of AI on social marketing and its usage in social media: A review analysis. In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE.
47. Baruah, A., Kumar, R., & Gupta, M. (2023, April). Analysis of Traffic Sign Recognition for Automated Transportation Systems Using Neural Networks. In *2023 IEEE 8th International Conference for Convergence in Technology (I2CT)* (pp. 1-5). IEEE.

ANTICIPATING BOSOM MALIGNANT GROWTH UTILIZING TROUPE AI MODELS

Abhay Kumar Pandey[1], Naman Tiwari [2], Swati Singh[3], Vineet Kumar Singh[4]

[1,2]Department of Computer Science and Engineering, IEC College of Engineering & Technology, Greater Noida, U.P., India.
[3]Department of Computer Science and Engineering, IMS Engineering College, Ghaziabad, UP, India
[4]Department of CSE-AI, ABES Institute of Technology, Ghaziabad-201009, UP, India
Email-Id: abhay.r2021@gmail.com, tiwarinaman675@gmail.com, swatisingh09.in@gmail.com, vineet.jpgc@gmail.com

Corresponding Author:abhay.r2021@gmail.com

Abstract— Early detection of breast cancer significantly increases treatment success and survival rates. Machine learning techniques offer promising tools for predicting breast cancer based on clinical data. This research explores the effectiveness of multiple machine learning models Support Vector Machines (SVM), Random Forest, Bagging, and AdaBoost classifiers for predicting breast cancer. Using a dataset containing features extracted from breast cancer cell nuclei, we preprocess the data by encoding target variables, handling missing values, and removing outliers. Model performance is evaluated based on accuracy, precision, recall, and F1 score. Our findings show that ensemble learning techniques, particularly the Random Forest and AdaBoost classifiers, outperformed other models, demonstrating high accuracy in breast cancer prediction. These results suggest that ensemble methods provide robust predictive models for early diagnosis in healthcare settings.

Keywords— Breast Cancer Prediction, Machine Learning, SVM, Random Forest, AdaBoost, Bagging Classifier, Ensemble Learning, Classification Models, Medical Diagnosis, Healthcare

I. INTRODUCTION

Bosom disease is quite possibly of the most well-known malignant growth influencing ladies around the world. Consistently, a huge number of new instances of malignant growth are analyzed universally, and further developing endurance rates generally depends on early finding. Precisely recognizing bosom growths as harmless or threatening is fundamental for settling on instructed treatment choices. Indeed, even in situations when traditional symptomatic strategies show compelling, they can be improved by the use of AI procedures that can deal with tremendous measures of clinical information to deliver forecasts in an opportune and dependable way. Bosom disease is perhaps of the most widely recognized sickness influencing ladies overall and is as yet a significant worldwide medical condition. As per expectations from the World Wellbeing Association (WHO), there were around 2.3 million new cases and 685,000 passings from bosom disease in 2020 alone. Early identification of bosom disease is significant for expanding endurance rates and offering effective treatment. While conventional symptomatic procedures like as ultrasonography, biopsies, and mammography stay essential in the clinical setting, headways in information driven advances have opened up better approaches to work on early location, determination, and guess. AI is one such headway in man-made consciousness (artificial intelligence) that has shown extraordinary commitment in the field of medical services, especially in the recognizable proof and forecast of disease. This kind of disease starts in the cells that make up the bosom tissue. It is portrayed by unusual cells multiplying wild, which may ultimately spread to other body regions in the event that treatment isn't finished. Bosom disease can introduce itself in a few structures, for example, ductal carcinoma in situ (DCIS), which is confined to the milk pipes, and obtrusive bosom malignant growth, in which malignant growth cells penetrate encompassing organs.

Bosom tissue thickening or knots, changes in the size or state of the bosoms, and uncommon release from the areolas are the most predominant indications of bosom disease. The way that numerous people, notwithstanding, stay asymptomatic in the beginning phases highlights the need of early ID and screening. The field of computerized reasoning known as AI (ML) centers around creating calculations that can recognize designs in information and use that information to gauge or decide. ML calculations consequently gain from past information, in contrast to conventional programming, to find examples and relationships that can then be applied to new, obscure information. Traditional programming gives the PC clear guidelines to adhere to. The utilization of AI in clinical analysis, particularly malignant growth location, is quickly getting some forward momentum on the grounds that to the overflow of clinical information accessible and headways in figuring power.

Histology data, sub-atomic profiles, and mammography pictures are a portion of the clinical and symptomatic datasets utilized in the preparation of AI models that expect bosom malignant growth. These datasets commonly incorporate marked examples, where each example is classified as harmless (not dangerous) or threatening (destructive). The AI model gains from these examples and makes an expectation model that can order beforehand obscure information in view of the examples it has distinguished. The objective is to make a model that can recognize harmless and dangerous growths precisely, helping clinical experts in the early identification of bosom disease. As of late, AI has demonstrated to be a useful technique for distinguishing clinical issues. By utilizing authentic information, models can anticipate the course of infections, which could prompt superior treatment plan improvement and early location rates. In the occasion of bosom disease, order models that separate among harmless and dangerous cancers might be developed in light of cell highlights. A few calculations, including SVM, Irregular Backwoods, and outfit techniques like Packing and AdaBoost, have been utilized to foresee bosom malignant growth, with differing levels of progress. This study expects to evaluate the prescient force of a few AI calculations for bosom disease. We utilize preprocessing strategies to clean and set up a dataset of bosom malignant growth cell cores credits prior to providing it to a few classifiers. We want to utilize execution measurements, for example, F1 score, exactness, accuracy, and review to figure out which model is doing awesome.

II. RELATED WORKS

On account of progressions in information driven innovation, the utilization of AI to distinguish bosom malignant growth has filled in prevalence as of late. Numerous scientists have taken a gander at different techniques, models, and procedures to build the precision and unwavering quality of bosom disease finding. It led a far reaching study surveying the viability of many models to gauge bosom disease utilizing a scope of AI draws near. Their examination features the need of assessing many AI ways to deal with distinguish the best models for a specific dataset. This near investigation might be utilized as an establishment for future examination to choose the best methodologies relying upon the accessible information and setting [1]. By contrasting the prescient force of a few AI models for bosom malignant growth. Their examination exhibited how cutting-edge AI strategies might be utilized to precisely recognize disease, especially in pragmatic settings like the World artificial intelligence IoT Congress [2]. They accomplished this by utilizing models that focused on presentation assessment to increment exactness. It joined small needle goal qualities, upsampling, and directed AI in an extraordinary way. Their examination offered new systems for further developing expectation exactness, particularly while working with imbalanced datasets. This approach stresses the meaning of preprocessing methods in AI assignments, especially as to taking care of inconsistent information conveyances [3]. To foster a half and half AI model that incorporates a few algorithmic methods to further develop forecast precision and empower fast bosom malignant growth expectation. Their work featured the need of making crossover models to make up for the constraints of individual calculations, which will add to the advancement of more precise bosom disease symptomatic frameworks [4]. to assess the expectation abilities of various AI calculations for bosom malignant growth by looking at evaluations of notable models. Their examination accentuates the meaning of calculation determination and model change to increment forecast exactness, which is in accordance with prior discoveries [5].

It proposed an AI based symptomatic strategy that utilizes highlight improvement procedures. The field's general propensity, which keeps up with that component designing is essential to working on the presentation of AI models for the determination of bosom disease, is predictable with their emphasis on highlight choice advancement [6]. A gated mindful multimodal profound learning way to deal with bosom malignant growth expectation was acquainted [7][11] with exhibit how profound gaining models can separate important experiences from complex, multimodal datasets where exceptional structures and information taking care of methods fundamentally affect model execution. By giving a complete examination of AI strategies used in bosom malignant growth expectation, it stressed the meaning of algorithmic determination. Their review works on past examination by offering an exhaustive viewpoint on many AI models and their exceptional advantages with regards to bosom disease forecast [8]. the conversation by exploring AI techniques planned explicitly for bosom malignant growth location and expectation. By showing what algorithmic improvements could straightforwardly mean for medical services applications, their review develops earlier examination on model execution [9].

It presented a clever profound learning model for the computerized location and classification of bosom malignant growth utilizing move learning strategies. Their methodology presents a new viewpoint on profound learning-based strategies by underlining how pre-prepared models might build the exactness of bosom disease forecasts, particularly when information shortage is a worry [10]. Bosom malignant growth is analyzed and distinguished utilizing CNN and MLP. their discoveries, which accentuate the utilization of profound learning methods. [11]. Profound learning-based advanced bosom tomosynthesis for robotized bosom malignant growth recognition. Their appraisal offers experiences into the cutting edge profound learning strategies used in clinical imaging, notwithstanding the mechanical progressions depicted by [12].[16]. an intensive assessment of PC supported symptomatic (computer aided design) strategies for the determination of bosom disease utilizing mammography. Various AI calculations for the expectation of bosom disease still intensely depend on computer aided design frameworks since they stay a fundamental piece of momentum research. [13]. It offered a near examination of bosom disease identification strategies utilizing information perception and AI innovation, underlining how representation helps with understanding information patterns and improves model execution. To overcome any issues between information show and AI, our review features the need of approving model expectations [14]. It supported the similar assessment of AI methods for bosom malignant growth expectation by giving an outline of many models and their adequacy in different settings. Their review proceeds with the act of benchmarking various methodologies, much as the relative examination [15][7]. By offering a near assessment of AI strategies for bosom disease expectation, it added to the developing collection of exploration that underscores the significance of model examination and assessment [16]. It analyzed profound learning and AI techniques for bosom malignant growth expectation, featuring the potential for further developing expectation results by consolidating cutting edge profound learning strategies with customary AI [17]. In light of everything, these examinations show the significance of component choice, model improvement, and algorithmic variety in further developing the expectation exactness of bosom malignant growth. They give a strong groundwork to future examination pointed toward improving AI based bosom disease recognition frameworks.

III. PROPOSED MODEL

Timely and precise disease identification is vital. This research focuses on Breast cancer prediction to improve detection precision and efficiency.

This methodology section details steps for covering experimental setup, data preprocessing, and evaluation metrics. Later sections elaborate on each aspect for comprehensive understanding.

A. Data Collection

The dataset utilized in this study contains estimations from bosom disease cell cores, including 30 highlights that depict different properties like sweep, surface, border, region, and perfection. The objective variable, determination, addresses whether the cancer is harmless (B) or threatening (M).

B. Data Preprocessing

We first load the dataset and conduct exploratory data analysis (EDA) to understand the structure and distribution of the data. Unnecessary columns, such as id and Unnamed: 32, are removed, and the target variable is encoded as a binary variable (0 for benign and 1 for malignant).

Before training the models, the dataset undergoes several preprocessing steps:

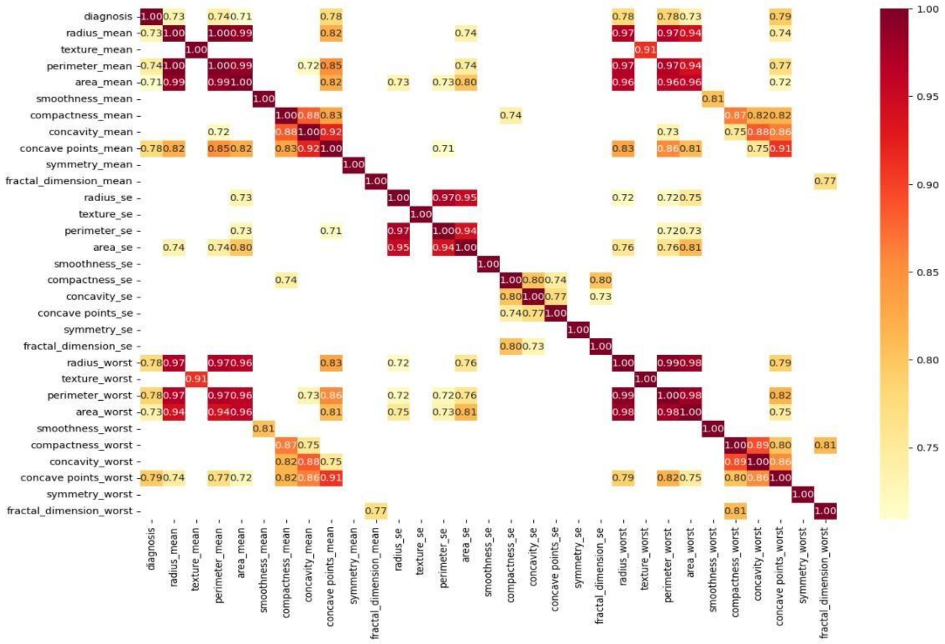
a) *Missing Values:* A check for missing values is performed, and no significant missing data is found in this case.

b) *Feature Scaling:* Since machine learning models like SVM are sensitive to feature scaling, we apply StandardScaler to normalize the feature values.

c) *Outlier Removal:* To ensure that extreme values do not distort the model's learning process, outliers are clipped based on the 1st and 99th percentiles of the feature distributions.

C. Exploratory Data Analysis

A correlation matrix highlights relationships between features, with some exhibiting strong correlations (greater than 0.7). This is an important step in understanding how different features might influence the models' predictions.



D. Model Selection

We evaluate the following machine learning models for breast cancer prediction:

a) *SVM:* An effective classification model for determining the best hyperplane to divide classes. The hyperplane's goal is to divide the data into two classes as best it can. The issue with optimization is:

b) *Random Forest Classifier:* The Random Forest method constructs several decision trees and compiles the outcomes. A portion of the data is used to construct each decision tree T_i. The majority vote (classification) from every tree determines the final prediction:

$$\hat{y} = mode(T_1(x), T_2(x), \ldots, T_N(x))$$

c) *Bagging Classifier:* Another ensemble method that combines multiple models to reduce variance and prevent overfitting.

d) *AdaBoost Classifier:* A boosting technique that focuses on correcting the errors of weak classifiers, progressively improving model performance. AdaBoost improves the performance of weak classifiers by adjusting their weights based on the errors. The weight update rule is:

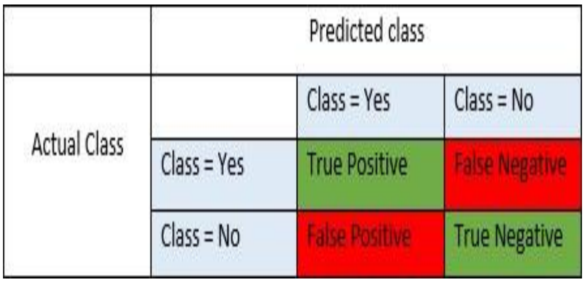
$$w_{i+1} = w_i \times e_{(\alpha\times 1(y_i \neq h(x_i)))}$$

Where, w_i is the weight of the i-th sample and α is the learning rate.

To guarantee reliable performance, the dataset is divided into training and testing sets (70% training, 30% testing), and 10-fold cross-validation is used to train the models.

E. Evaluation Matrices

A performance measure provides a basis for quantitative analysis. It is a scale to measure the quality against the desired goal. The following well-known metrics is predominantly used for evaluation of model:



	Predicted class		
Actual Class		Class = Yes	Class = No
	Class = Yes	True Positive	False Negative
	Class = No	False Positive	True Negative

TABLE I. CONFUSION MATRIX

Assessing the efficiency of a ML model, particularly in classification tasks, is significantly influenced by the importance of *evaluation metrics*. These metrics offer quantitative measures that gauge the model's performance in correctly categorizing instances into different classes. In a classification context, Common metrics include *accuracy, precision, F1 score, and recall [18][19].*

a) Accuracy: It is the most typical metric for determining the accuracy for any classification approach. It can be measured as the proportion of reviews that are correctly categorized to all reviews. The below mentioned formula will be utilized to found accuracy [20][21]:

$$\boldsymbol{Accurarcy = (TP + TN)/(TP + TN + FP + FN)} \qquad \textbf{(1)}$$

a) Precision: Precision, in classification, measures the model's accuracy specifically in predicting positive outcomes. It is seen as the assessment size of a classifier's exactness. Low precision can show a tremendous number of counterfeits up-sides. The significance and exercise of "exactness" is different while portraying rightness and precision in additional pieces of authority and data. The formula for precision is [22]:

$$\boldsymbol{Precision = TP/(TP + FP)} \qquad \textbf{(2)}$$

b) Recall (Sensitivity or True Positive Rate): In classification, recall evaluates a model's ability to accurately identify all relevant cases within a particular category, measuring true positives against the total actual positives. The formula for recall is:

$$\boldsymbol{Recall = FN/(TP + FN)} \qquad \textbf{(3)}$$

c) F1 Score: It is an important accuracy measure technique and is used when the distribution of positive labeled data and negative labeled data is uneven. It varies between 0 and 1, with higher values indicating a more balanced performance. So, whenever a model is prepared, the confusion matrix has to be prepared as shown table 1.1 that evaluates the precision and recall and by using precision and recall value, we can easily calculate F1-score.The formula for F1 score is:

$$\boldsymbol{F1\ Score = (2 * Recall * Precison)/(Recall + Precison)} \qquad \textbf{(4)}$$

IV. RESULTS AND DISCUSSION

Exactness, accuracy, review, and F1 score are among the presentation markers used to survey the models. An outline of the results for each model is displayed beneath: SVM: The SVM model had a reduced recall for malignant patients and suffered with class imbalance, despite achieving a respectable level of accuracy. Random Forest: This model demonstrated remarkable performance, with excellent recall, accuracy, and precision. The Random Forest's strong performance was a result of its capacity to manage the dataset's variability and feature relevance. Bagging: By minimizing overfitting and producing reliable predictions, the Bagging classifier also demonstrated competitive performance. AdaBoost: AdaBoost fared better than SVM and Bagging in terms of F1 score and recall, and it was especially good at detecting malignant tumors.

TABLE I Output After Encryption

Model	ROC Score	Precision Score	Recall Score	F1 Score	Accuracy Score
Support Vector Machine	0.957955	0.980769	0.927273	0.953271	0.965035
Adaboost Classifier	0.961364	0.962963	0.945455	0.954128	0.965035
Random Forest Classifier	0.946591	0.944444	0.927273	0.935780	0.951049
Bagging Classifier	0.922727	0.924528	0.890909	0.907407	0.930070

The performance comparison of four models—SVM, AdaBoost, Random Forest, and Bagging Classifier—shows that: AdaBoost and SVM deliver the highest accuracy (96.5%) and strong F1 scores (0.954 and 0.953, respectively). AdaBoost slightly outperforms SVM with a higher ROC score (0.961) and recall (0.945), making it the best overall model. Random Forest follows with an accuracy of 95.1% and a good balance of precision (0.944) and recall (0.927). Bagging Classifier shows the lowest performance, with a 93.0% accuracy and lower recall (0.891) compared to the other models. Overall, AdaBoost is the top-performing model for breast cancer prediction, followed closely by SVM.

V. FUTURE SCOPE

The use of machine learning techniques has enormous promise for the future, as seen by the implementation for breast cancer prediction that was presented. The efficacy, scalability, and generalizability of the models employed in this work can be improved by investigating a number of areas. Key elements of the research's future scope are delineated in the sections that follow, including the use of sophisticated machine learning techniques, data diversity, interpretability, model optimization, and interaction with clinical practice. There are many prospects for enhancing model performance, interpretability, and practical applicability in the broad future of machine learning for breast cancer prediction. Improvements in data science, artificial intelligence, and medical research will probably result in more precise, individualized, and effective diagnostic tools as this sector develops. Future examinations can help effectively incorporate AI into clinical work on, working on persistent results and changing the finding and therapy of bosom malignant growth by handling present issues like model enhancement, information variety, and moral contemplations.

VI. CONCLUSION

This study shows the adequacy of AI models, especially troupe strategies, in anticipating bosom malignant growth. Random Forest and AdaBoost classifiers arose as the best entertainers, offering high exactness and dependability in recognizing harmless and dangerous cancers. These models can be coordinated into medical care frameworks to help clinicians in early determination, possibly working on quiet results.

Future research can explore more advanced techniques, such as deep learning models, and assess their effectiveness on larger and more diverse datasets. Additionally, fine-tuning model parameters and incorporating real-world clinical data may further improve predictive accuracy.

REFERENCES

[1] Bhanushali, A., Sivagnanam, K., Singh, K., Mittapally, B. K., Reddi, L. T., & Bhanushali, P. (2023). Analysis of breast cancer prediction using multiple machine learning methodologies. International Journal of Intelligent Systems and Applications in Engineering, 11(3), 1077-1084.

[2] Liza, F. T., Das, M. C., Pandit, P. P., Farjana, A., Islam, A. M., & Tabassum, F. (2023). Machine learning-based relative performance analysis for breast cancer prediction. In 2023 IEEE World AI IoT Congress (AIIoT) (pp. 0007-0012). IEEE.

[3] Shafique, R., Rustam, F., Choi, G. S., Díez, I. de la T., Mahmood, A., Lipari, V., Velasco, C. L. R., & Ashraf, I. (2023). Breast cancer prediction using fine needle aspiration features and upsampling with supervised machine learning. Cancers, 15(3), 681.

[4] Dalal, S., Onyema, E. M., Kumar, P., Maryann, D. C., Roselyn, A. O., & Obichili, M. I. (2023). A hybrid machine learning model for timely prediction of breast cancer. International Journal of Modeling, Simulation, and Scientific Computing, 14(4), 2341023.

[5] Ebrahim, M., Sedky, A. A. H., & Mesbah, S. (2023). Accuracy assessment of machine learning algorithms used to predict breast cancer. Data, 8(2), 35.

[6] Uddin, K. M. M., Biswas, N., Rikta, S. T., & Dey, S. K. (2023). Machine learning-based diagnosis of breast cancer utilizing feature optimization technique. Computer Methods and Programs in Biomedicine Update, 3, 100098.

[7] Kayikci, T., & Khoshgoftaar, T. M. (2023). Breast cancer prediction using gated attentive multimodal deep learning. Journal of Big Data, 10(1). https://doi.org/10.1186/s40537-023-00749-w

[8] Nemade, V., & Fegade, V. (2023). Machine learning techniques for breast cancer prediction. Procedia Computer Science, 218, 1314–1320. https://doi.org/10.1016/j.procs.2023.01.110

[9] Naji, M. A., Filali, S. E., Aarika, K., Benlahmar, E. H., Abdelouhahid, R. A., & Debauche, O. (2021). Machine learning algorithms for breast cancer prediction and diagnosis. Procedia Computer Science, 191, 487–492. https://doi.org/10.1016/j.procs.2021.07.062

[10] Saber, A., Sakr, M., Abo-Seida, O. M., Keshk, A., & Chen, H. (2021). A novel deep-learning model for automatic detection and classification of breast cancer using the transfer-learning technique. IEEE Access, 9, 71194–71209. https://doi.org/10.1109/access.2021.3079204

[11] Desai, M., & Shah, M. (2021). An anatomization on breast cancer detection and diagnosis employing multi-layer perceptron neural network (MLP) and convolutional neural network (CNN). Clinical eHealth, 4, 1–11. https://doi.org/10.1016/j.ceh.2020.11.002

[12] Bai, J., Posner, R., Wanga, T., Yang, C., & Nabavi, S. (2021). Applying deep learning in digital breast tomosynthesis for automatic breast cancer detection: A review. Medical Image Analysis, 71, 102382.

[13] Ramadan, S. Z. (2020). Methods used in computer-aided diagnosis for breast cancer detection using mammograms: A review. Journal of Healthcare Engineering, 2020, 9162464. https://doi.org/10.1155/2020/9162464

[14] Ak, M. F. (2020). A comparative analysis of breast cancer detection and diagnosis using data visualization and machine learning applications. Healthcare, 8(2), 111. https://doi.org/10.3390/healthcare8020111

[15] Islam, M. M., Haque, M. R., Iqbal, H., Hasan, M. M., Hasan, M., & Kabir, M. N. (2020). Breast cancer prediction: A comparative study using machine learning techniques. SN Computer Science, 1, 1-14.

[16] Fatima, N., Liu, L., Hong, S., & Ahmed, H. (2020). Prediction of breast cancer, comparative review of machine learning techniques, and their analysis. IEEE Access, 8, 150360-150376.

[17] Tiwari, M., Bharuka, R., Shah, P., & Lokare, R. (2020). Breast cancer prediction using deep learning and machine learning techniques. Available at SSRN 3558786.

[18] Gupta, M., Kumar, R., & Abraham, A. (2024). Adversarial Network-Based Classification for Alzheimer's Disease Using Multimodal Brain Images: A Critical Analysis. *IEEE Access*.

[19] Yadav, A., Kumar, R., & Gupta, M. (2024, March). An analysis of convolutional neural network and conventional machine learning for multiclass brain tumor detection. In *AIP Conference Proceedings* (Vol. 3072, No. 1). AIP Publishing.

[20] Kaur, R., Kumar, R., & Gupta, M. (2024). Lifestyle and Dietary Management Associated with Chronic Diseases in Women Using Deep Learning. *Combating Women's Health Issues with Machine Learning*, 59-73.

[21] Juneja, A., Kumar, R., & Gupta, M. (2022, July). Smart Healthcare Ecosystems backed by IoT and Connected Biomedical Technologies. In *2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 230-235). IEEE.

[22] Gupta, M., Chaudhary, G., Bansal, D., & Pandey, S. (2022). DTLMV2—A real-time deep transfer learning mask classifier for overcrowded spaces. *Applied Soft Computing*, *127*, 109313.

SMART GRID WITH INTERNET OF THINGS APPLICATIONS

Ramiz Salama[1*], **Fadi Al-Turjman**[2, 3]

[1]Department of Computer Engineering, AI and Robotics Institute, Research Center for AI and IoT,
Near East University Nicosia, Mersin 10, Turkey
[2]Artificial Intelligence, Software, and Information Systems Engineering Departments, AI and Robotics Institute,
Near East University, Nicosia, Mersin10, Turkey
[3]Research Center for AI and IoT, Faculty of Engineering, University of Kyrenia, Kyrenia, Mersin10, Turkey

*Corresponding author Email: ramiz.salama@neu.edu.tr

ABSTRACT

The smart grid, an updated energy infrastructure using cutting-edge communication and information technology, is replacing traditional power grids. The Power Internet of Things (PIoT) integration enhances efficiency by managing informational flows in tandem with inherent energy fluxes throughout transmission, distribution, or generation processes. This article argues in favor of incorporating new revenue streams into existing smart grids, highlighting the untapped potential of innovative services and market mechanisms, and enhancing efficiency through the exchange of valuable data to supplement scarce resources and the latest 5G advancements. The Savvy Network (SG) concept aimed to change how the electrical matrix base and capabilities were managed by the flow framework. The Sharp Lattice perspective was added to the conventional power structure to improve the way that age, transmission, and flow networks interact together. However, more advanced features like programmed directionality, safety, adaptability, self-healing and mindfulness, continual assessment, and layer-to-layer commonality are not included in either the current or previous conceptions of smart networks. The future Massive Internet of Things (MIoT) is one of the main components of the 5G/6G network factory. This study investigates the architecture and issues of the future generation of smart grids, focusing on AI-powered smart grids and the integration of AI, IoT, and 5G, to improve smart grids. The smart grid is a new development in science and innovation that has increased vulnerability to hackers. This article provides an overview of the security considerations of IoT-backed smart grids, highlighting the potential benefits of incorporating new revenue streams, innovative services, and market mechanisms.

Keyword: clever structure, frameworks of power, network of things safeguarding digital content, Digital attack, Break detection, Interruption detection.

1. Introduction

Brilliant networks will be the cutting edge of the energy structure. The energy frameworks that are in place now coordinate smart meters, sensors, and high-level registering technologies. Combining several power sources into a single system can boost power generating efficiency, thanks to smart grid technologies. Power producing centers have real-time data on electricity consumption because smart meters and sensors are connected to the grid. With this understanding, effective creation and dissemination methods can be implemented. When these technologies are included into the architecture of the energy system, energy efficiency rises dramatically and power prices fall. A few nations are making investments in swift framework enhancement as a result of stretching the bounds of what qualifies as extraordinary societal and financial benefits. In any case, communication networks present security risks and are vulnerable to cyberattacks. Because of this, it is essential to include online security and digital threat detection while creating smart networks. The Public Organization of Principles and Innovation (NIST), the Energy Master Digital protection Stage (EESCP), and the Savvy Matrix Team of the European Commission underscore the significance of network safety in the future stunning lattice improvements.

Since then, a number of audits that recommended network security measures and provided proof of electronic interruption detection have been followed up on. A robust system architecture integrates several resources and cutting-edge technology. Brilliant meters increase the productivity of the dispersion framework by gathering utilization data. Moreover, SCADA, which combines administrative control and data collection, assumes a longer and more concentrated dispersion over broad geological horizons. Smart grids can be linked to transmission and diversion frameworks, building regulators, energy-age sources, and other components [1–5]. On the other hand, modern networks grow more complex and vulnerable to distributed computing failures and attacks when they integrate information technologies and computational procedures. Consequently, the organization assurance of the insightful structure faces numerous obstacles. The complexity of expressing the likelihood hypothesis, the structure's nonlinearity, and the range of sophisticated attacks that could compromise the system are all included in two of his models. A subset of highly skilled risk specialists and hacker groups concentrate on critical systems and organizations, ranging from basic security architectures to intelligent enterprises and clinical advantages. is speculating.

Moreover, the Web of Things (IoT) innovation has expanded into a real-world collection of online-connected objects. By supporting various operations of the generation and storage network and enabling connectivity between providers and customers, the deployment of such devices can assist the smart grid. Cyberattacks are more likely to occur when Internet of Things (IoT) devices are integrated into smart grids. The literature suggests a wide range of methods for spotting cyberattacks. Model-based solutions include statistical models and variants on state estimation techniques. Moreover, Kalman filtering has been suggested as an estimation assessment technique for cyberattack detection. However, a useful framework was also mentioned. It has been suggested that supervised learning be used to identify fraudulent data injection attacks (FDI). Semi-supervised machine learning techniques, for example, can benefit from the geographical and temporal correlation of smart meter information, while supervised machine learning approaches offer greater precision. Deep learning and incentive learning schemes are just two of the many artificial intelligence-based programs that have been released.

Suggested combining Fake Insusceptible Frameworks (AIS) with Backing Vector Machines (SVM) to identify fraudulent data. advises, on the other hand, that stretch states be advanced. a protection system that uses deep learning to recognize nonlinear features by extracting approximations from electric load data. Regularly detecting false information injection attempts is another application of profound learning. To lessen cyberattacks, real-time PMU metrics are also evaluated using deep learning. Suggests using a Repetitive Brain Organization (RNN) to find digital attacks and discover temporal abnormalities within gradually confirmed data. further proposes the use of self-supervised deep learning to create a versatile intelligent assault detection system. Medication, the Health System, and Insightful Organizations are just a few of the companies and associations that programming teams and other major level risk takers have recognized. Numerous solutions have been developed in response to the variety and complexity of cyber threats to the smart grid. For shrewd lattices, therefore, a bibliographic analysis and a synopsis of the most recent network security methods are crucial. Moreover, there isn't a similar analysis in the literature. On this topic, numerous research articles and abstracts have already been published. For instance, fake organizational security summaries and assessments are offered. An additional important study on efficient digital real framework planning. But as these reports were all written before 2016, they are out of current and do not incorporate many of the most recent recommendations for changes. Subsequently, the authors published their written assessment reports, which examined various computer-related risks within this large organization. However, none of the studies examined the assault detection techniques used or conducted a bibliographic study of the relevant literature. A summary of articles on network health using the logical framework is provided [6–10]. They focus on cybersecurity regulations, but they don't disclose the kinds of cyberattacks that are carried out or the protections that are put in place.

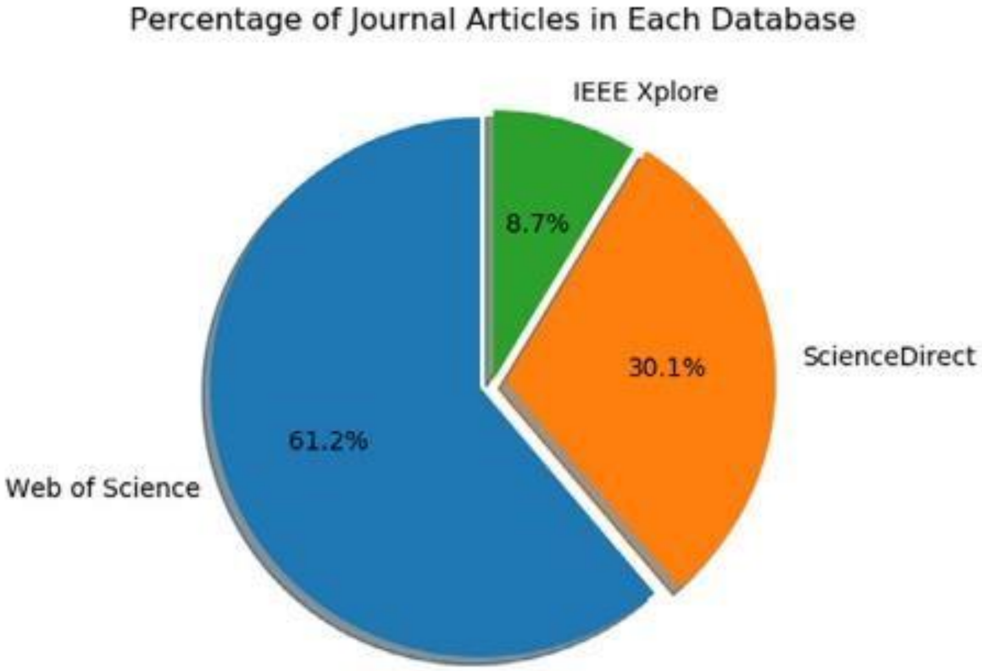


Figure 1: Percentage of journal articles published in each database on the topic of security systems in the smart grid.

Since its introduction to the world till now, the energy age, or the principles of transmission and circulation, have undergone several modifications and improvements. A decentralized worldview is replacing the power era's highly centralized one. Traditional power grid structures cannot handle new demands like robotic error and randomness checks, more efficient transmission, and problems with sustainable system combinations. To address the needs and difficulties, the Shrewd Matrix (SG) idea was created. Further improvements to the electrical lattice for SG require several changes to charge choices and innovations in stream networks. The main concept was to enhance the functionality, durability, and dependability of electrical structures by utilizing data and communication advancements.

The idea of smart metering (SM) is maybe his most significant development that empowers SG. In addition to providing accurate, automatic, and regular dissemination of information about customers' energy use, smart meters (SMes) enable two-way communication channels between utility companies and customers. is swappable. Customers and specialty co-ops both gain from this. For example, energy costs force customers to change their workout routines, but suppliers benefit from remote inspection, planning, separation/migration, diagnostics, blackout identification, authoritative issues, and setting the board goal. can benefit from cutting back on expenses. [Four]. Because each Assignment Structure Director (DSO) makes unique mechanical and budgetary decisions, the existing situation is inconsistent. To make these much-needed adjustments, there are still some obstacles to be solved. It's connected to specialized communications engineering to some extent. This provides basic requirements like accessibility and adaptability with consistent quality and allows for the authorized transmission of information in a variety of environments, including urban and rural ones. There isn't a correspondence convention or environment that works for everyone because they all have pros and cons of their own.

An illustration of the SG and SM conditions influencing the enhancement of the SM system is provided in this article. We outline specific methods to enhance the lattice behavior in super grids. We discuss how SM foundations might develop in the future while keeping IoT standards in mind. We also concentrate on SM frameworks to investigate potential applications of Web of Things (IoT) conventions in SG settings. Here, we propose a novel strategy that makes use of the Internet of Things. The main goal is to suggest the use of IoT-enabled advancement in the context of SM and to focus on possible enhancements in comparison to the current state of advancement. We are wondering how we may deploy autonomous aerial vehicles (UAVs) in remote and rural areas where alternative communication breakthroughs are likely unimaginable or prohibitively expensive, given the apparent lack of a suitable framework for media transmission [11–15]. We'll look into whether it can be used to increase the functionality of the program. The first results from fieldwork in real life demonstrate the viability of the proposed solution.

2. RELATED WORK

A group of blocks with identical records and structures is called a blockchain. Correlated blocks exist. Block connections could be broken by minor modifications to the records inside those blocks. It is sometimes referred to as state machine replication since the blockchain is replicated across a collection of hubs, each of which shares a section of the organization. has a total of two blockchain classifications. blockchain with or without permission. Both the entire public and specific entities verify transactions on the permission-less blockchain. Conventional systems are more centralized but also speedier and more scalable. On the other hand, anyone can access a blockchain system without permission.At the time of generation, blockchain data cannot be changed. The Bitcoin framework has been considered in over 80% of documents; less than 20% of contracts containing other blockchain applications, like permissions and smart contracts, include this feature.

Most publications attempt to draw attention to blockchain systems' inefficiencies as well as their privacy and security flaws. However, there is no concrete evidence or a clear picture to support their claims. Some of the most significant blockchain protocols are examined by the authors. The developer showcased his Hyperledger blockchain architecture, a popular open-source system with many pluggable features due to its design. By offering a publicly accessible platform for transmitted data upkeep, you may promote blockchain innovation. This Linux-based era has the potential to drastically change the industry's character. In fact, his Hyperledger is used by many of the blockchain solutions available on the market. Explains how IoT and blockchain technologies can be combined to address a range of problems and application cases. The majority of research has been on the shared digital economy's applications. Additionally, several models are carefully crafted for the development of blockchain and the Internet of Things. The authors proposed a method of recording. Data pertaining to medicinal treatments is obtained through haze calculations. We suggest a blockchain architecture that will enable the methods outlined in this paper to be used for the collection and entry of medical records. In order for competent eHealth administrators to use turbidity calculations effectively, the authors are still trying to improve them. The author discusses the features, evolution, and history of the blockchain as well as its transformative impact on IT and non-IT companies. The authors conducted a thorough literature analysis in order to clearly and succinctly explain the concepts and implications of blockchain technology. The author provides a more thorough theoretical explanation of blockchain technology with a plethora of examples. The author talked about how the banking industry has improved security and privacy. Blockchain technology offers the banking sector a reliable means of incorporating security features while addressing the difficult problems of autonomous decentralized systems and permissionless systems.

Health Records, Health Systems, Health Care & System & Records, and Health Care Blockchain were the search terms used to find papers related to EHR literature searches from a variety of sources, including the ProQuest and Google Scholar databases. This text may provide a brief summary with only a few references to significant research papers. As technology advances, we must demonstrate that we are ready to preserve medical records. Getting physical copies is standard practice for 87% of Americans, and almost half of them receive these documents from medical professionals. However, a number of security-related problems with EHR systems make it difficult for people to share information. Rezaeibagha et al. looked at and studied the security and privacy issues with EHR systems.Integration and sharing of information has been found to have a major influence on privacy and security [16–20]. The efficacy of the EHR system was recently investigated by Afrizal et al. The examination encompassed both individual and organizational perspectives. Their investigation exposed organizational limitations and also pointed to a lack of skilled personnel, a lack of senior management, and a lack of teamwork. Lack of computer access and unfamiliarity with new software were examples of personal limitations.

New technologies are essential in removing these kinds of obstacles, and blockchain provides a number of solutions for lowering barriers in EHR systems. Blockchain technology allows for the reliable recording and unchangeable preservation of every transaction that occurs within a network. Furthermore, no one individual is responsible for overseeing the computing work required to carry out multi-computer transactional procedures due to the system's complete distribution. The application of blockchain technology holds potential for enhancing the United Nations' sustainable development goals, particularly in the healthcare sector. Electronic health records and other public sector services could be modernized with the use of blockchain technology. Secure data exchange settings show how the patient experience is prioritized, and Zhang and his colleagues looked into blockchain as a possible way to protect patient data in healthcare systems. One way to improve health information management is by using blockchain technology, which improves opioid prescription monitoring and makes it easier to access cancer patient records and other medical services like telemedicine and insurance access. It's a single. By examining patient health data, we demonstrated how blockchain is transforming the transmission of medical information. Multiple blocks with the same structure and information-recording capabilities make up a blockchain. Blocks are connected via links.

Depending on your input, you can break the links between those blocks by changing the data inside them. Since the blockchain is repeated across a network of nodes, each of which has a stake in the network, it is occasionally referred to as state machine replication. Blockchains fall into two major categories. blockchain, whether or not it is authorized. Both the entire public and specific entities verify transactions on the permissionless blockchain. Conventional systems are more centralized but also speedier and more scalable. On the other hand, anyone can access a blockchain system without permission. At the time of generation, blockchain data cannot be changed. The EMR monitoring products that are now on the market are described by the authors.The authors elaborate on their ongoing study on blockchain technology.

The generated numbers show how much work is being put into different blockchain application cases. The Bitcoin framework has been considered in over 80% of documents; less than 20% of contracts containing other blockchain applications, like permissions and smart contracts, include this feature. Most publications attempt to draw attention to blockchain systems' inefficiencies as well as their privacy and security flaws. However, there is no concrete evidence or a clear picture to support their claims. Some of the most significant blockchain protocols are examined by the authors. The developer showcased his Hyperledger blockchain architecture, a popular open-source system with many pluggable features due to its design. By offering a publicly accessible platform for transmitted data upkeep, you may promote blockchain innovation. This Linux-based era has the potential to drastically change the industry's character. In fact, his Hyperledger is used by many of the blockchain solutions available on the market.

The majority of research has been on the shared digital economy's applications. Additionally, many of the models are carefully crafted with blockchain and IoT development in mind. The authors proposed a method of recording. Data pertaining to medicinal treatments is obtained through haze calculations. The methodology proposed in this paper can be used to collect and enter medical records into our proposed blockchain framework. In order for competent eHealth administrators to manage turbidity computations effectively, the authors are now trying to enhance them. The author discusses the features, evolution, and history of the blockchain as well as its transformative impact on IT and non-IT companies. The authors conducted a thorough literature analysis in order to clearly and succinctly explain the concepts and implications of blockchain technology. The author provides a more thorough theoretical explanation of blockchain technology with a plethora of examples. The author talked about how the banking industry has improved security and privacy. Blockchain technology offers the banking sector a reliable means of implementing security features by addressing the intricate problems of autonomous decentralized systems and permissionless systems.

Although Zhang et al. praised a blockchain architecture as the best method for managing health information, there aren't many studies on it for patient records. One example of this is the proposal by Fan et al. for a blockchain-based management information system for EHRs in response to privacy and security concerns. The ledger database committer, ordered, endorser, and client are the six components that form the foundation of their design. The Fan-led group, however, paid little attention to the challenges around personal data or the concepts of digital currency [21–25]. They left these subjects for further research in order to aid Fan et al.'s efforts. In an effort to resolve security concerns that arose when utilizing blockchain, Griggs and colleagues worked on building a private network. Block can document J and K's past and present circumstances because of its longevity as a record-keeping tool. Sadeghi Instead, there are two categories of transactions: private and public. According to research by Griggs and other experts, private blockchains may be a useful tool for addressing privacy issues with the

way personal data is handled in the healthcare sector. Privacy concerns may have an impact on people's decision to regularly use EHR systems. In their study, Sharma and co-authors used the soft systems technique to qualitatively demonstrate that the adoption of blockchain technology for EHR sharing raises the percentage of patients who opt in. They concentrated on the Precision Health Care (PHC) initiative, which consists of a collection of separate EHRs designed to promote universal access and public health advancement. The blockchain-based system concept has been demonstrated to boost trust in unreliable PHC systems and promote better collaboration by offering enhanced access to patient records. Esmaeilzadeh and Mirzaei, researchers who examined the potential impact of blockchain on HIE, found that users would mostly choose a blockchain-based system because of its privacy-protecting capabilities. In order to simplify blockchain integration into EHR, Shahnaz and colleagues offered a way to resolve issues regarding flexibility during blockchain implementation by recommended structural changes. Future research may examine the various advantages and disadvantages of applying blockchain technology in the medical domain. This is the most significant study to date on the impact of blockchain technology on patients' plans to use mediation to exchange their healthcare data. The use of blockchain technology in healthcare is yet unknown, despite a number of recent research looking at how this technology might enhance health information administration. Due to a lack of research, we do not completely understand how security perceptions and extrinsic motivations affect the information systems that healthcare providers utilize.

3. TECHNIQUES

Determining the potential benefits and challenges of implementing blockchain technology in the healthcare industry is the aim of this study. The methodological technique utilized to conduct the inquiry is described in this section of the report. Fig.,

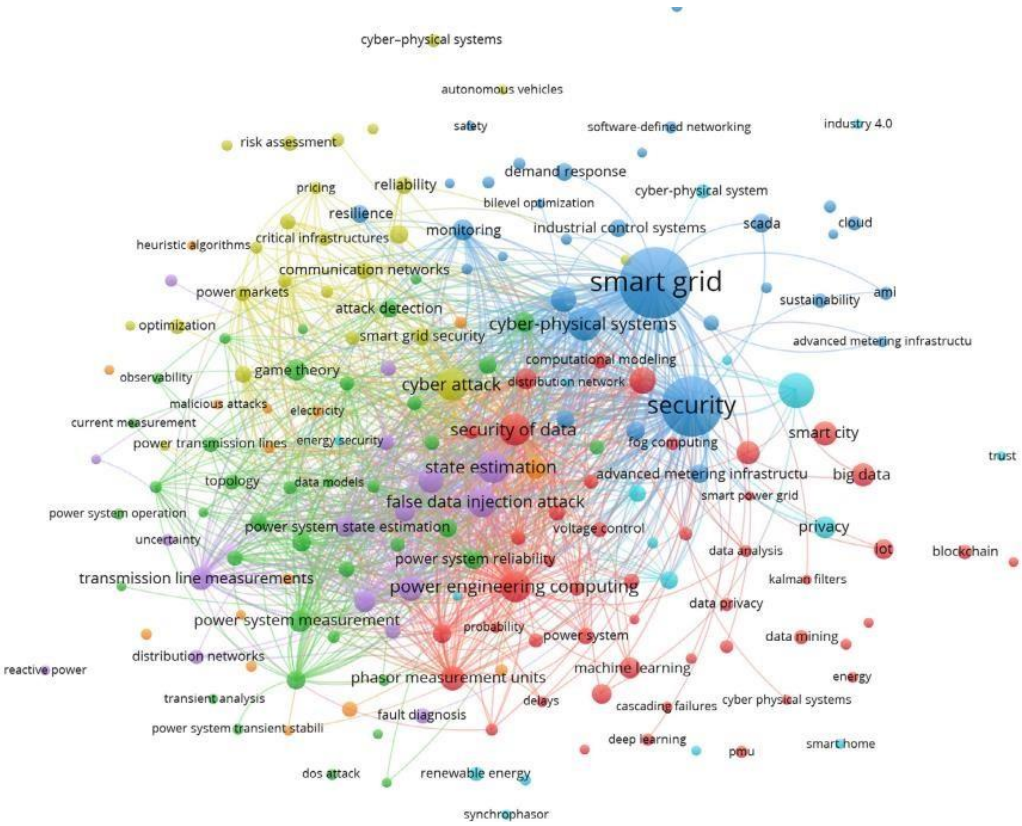


Figure 2: A heatmap of the terms used in every journal paper about cybersecurity for smart grids.

and in order to conduct this review, we followed four main procedures, which included extracting and pre-processing the data set as well as inspecting and interpreting it. If you want to learn more about the intersections between blockchain technology and the healthcare sector as documented by their indexation in WoS and Scopus between 2016 and 2020, go no further than this dataset. This study conducted a bibliometric examination of blockchain technology in the healthcare sector using the open-source statistics program R. The R desktop system has the software installed and is now in use [26–30]. Numerous academic fields have investigated this bibliometrics technique.

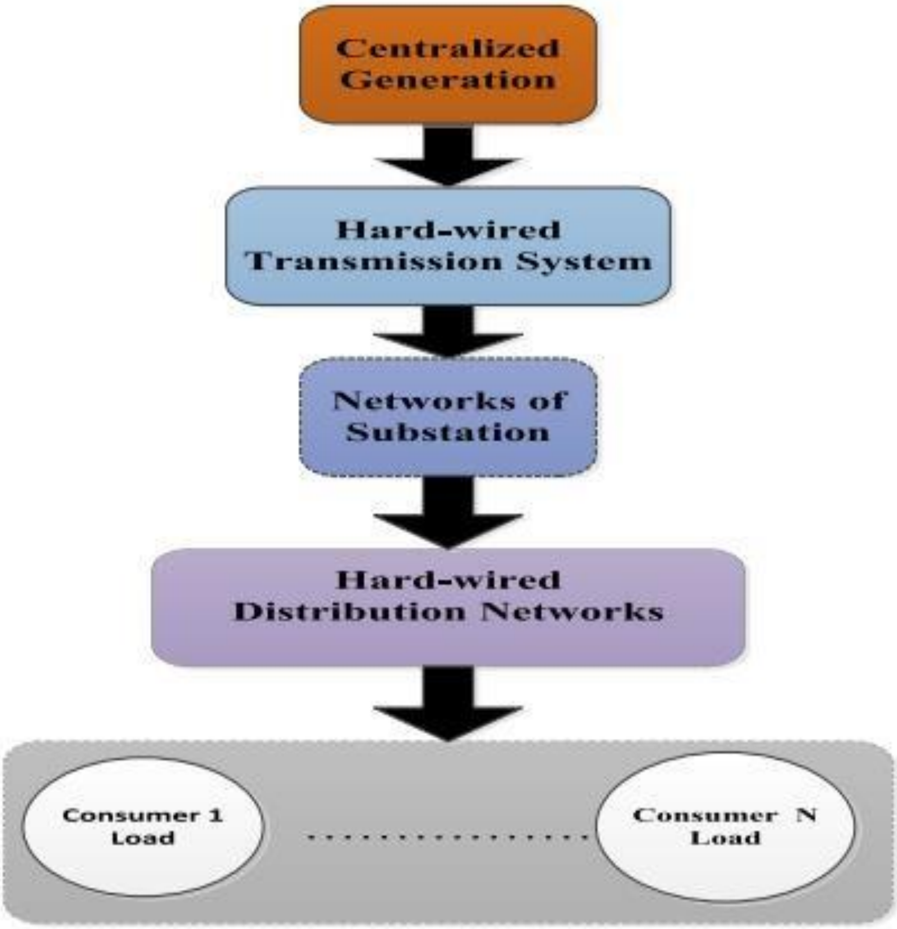


Figure 3: The classical grid block diagram.

In order to find articles that had the term "blockchain in medical services" in their titles, watchwords, or altered compositions, this paper conducted a literary survey. The evaluation of previous research aimed to identify blockchain applications in healthcare administration, or areas where its use has been proposed. A range of online resources, such as ResearchGate, Google Scholar, the EBSCO database, the Web of Science, and the Applied Science & Technology Source, were used to choose the publications. A review of the advantages and disadvantages of blockchain-based technology in the healthcare industry was conducted using forty of the most recent manuscripts from a selection of articles published between 2016 and 2020 [31–35]. Journals with a health focus were preferred, and only written works in the English language were taken into account. The poll's findings provide a thorough overview of blockchain's potential as well as a list of ways that it affects medical care associations' daily operations. The results also indicate that there is a dearth of research and application-based activity in the field.

4. **Real-world applications of the Internet of Things and smart grid**

By facilitating more effective and data-driven procedures, the Internet of Things (IoT) and smart grid applications are revolutionizing a number of industries. Here are some examples of how IoT and smart grid technologies are being used in the real world:

1. Intelligent Houses and Structures

- Use: Internet of Things-enabled smart lighting and thermostat systems (like Nest and Ecobee).

- Functionality: By connecting devices to a central hub, users may automate tasks like lighting and temperature control based on real-time data, optimize energy use, and remotely operate household appliances.
- Advantages include improved user convenience, cost savings, and increased energy efficiency.

2. Utilities Smart Meters

- Usage: Gas, electricity, and water smart meters.
- Functionality: Smart meters enable two-way communication between users and utilities as well as real-time monitoring. Utility firms utilize this information to optimize energy distribution and provide more accurate bills to customers.
- Advantages include better load balancing, fewer outages, and more precise pricing.

3. Energy Management using Smart Grid

- Use: Smart grid systems enabled by the Internet of Things (e.g., applied in cities like San Diego, Barcelona).
- Functionality: To minimize waste and boost efficiency, smart grids employ sensors and realtime data analytics to track the movement of electricity throughout the grid, identify malfunctions or outages, and optimize energy supply.
- Advantages include enhanced response times to electrical problems, more reliable electrical networks, and greater incorporation of renewable energy.

4. Intelligent Traffic Control

- Use: Internet of Things-based traffic monitoring and control systems (like Automated Traffic Surveillance and Control (ATSAC) in Los Angeles).
- Functionality: Cameras and sensors monitor traffic, accidents, and congestion; they automatically modify traffic signals and give drivers real-time information.
- Advantage: Better urban mobility, less pollution, and less traffic congestion.

5. Intelligent Farming • Use: Precision farming using Internet of Things sensors.

- Functionality: Field sensors gather information about crop conditions, temperature, and soil moisture. This information can be used by farmers to improve planting, harvesting, and irrigation.
- Advantage: Lower environmental impact, less water use, and higher crop output.

6. Integration of Renewable Energy into the Smart Grid

- Use: Internet of Things and microgrids for managing renewable energy (e.g., Siemens and ABB projects).
- Functionality: Smart grids control the distribution of energy produced by solar and wind power, while Internet of Things sensors monitor this production. It is possible to store excess energy or reintegrate it into the grid.
- Advantages include improved grid stability, less dependency on fossil fuels, and better integration of renewable energy.

7. Healthcare: Medical Devices Powered by IoT

- Use: Internet of Things in linked medical devices (e.g., heart monitors, smart insulin pens).
- Functionality: Health data is gathered in real time by devices and transmitted to healthcare providers. Alerts for appointments or medication can also be sent to patients.
- Advantages include early identification of possible health problems, remote monitoring, and better patient care.

8. Smart charging and electric cars (EVs)

- Use: EV charging stations with Internet of Things connectivity (e.g., ChargePoint).
- Functionality: Smart grid-connected charging stations modify charging schedules in response to energy pricing, grid demand, and renewable energy availability.
- Advantages include reduced grid stress, optimized energy use, and EV charging that incorporates renewable energy.

9. IoT for Energy Efficiency in Industry (IIoT)

- Use: Industrial energy management via the Internet of Things (e.g., Schneider Electric's EcoStruxure).
- Functionality: Sensors keep an eye on energy usage, machine performance, and the need for preventative maintenance.
- Advantages include lower energy expenses, better operational effectiveness, and less equipment downtime.

10. Smart Cities • Use: IoT deployments throughout the city (e.g., Barcelona's smart city initiative). • Functionality: Lighting, environmental monitoring, and waste collection are all managed via IoT devices. Real-time data is collected on energy use, air quality, and traffic flow.

- Advantages include more sustainable infrastructure, lower operating costs for cities, and better living conditions in metropolitan areas.

These uses show how IoT and smart grid technologies are changing services and industries to create more connected, sustainable, and efficient systems.

Applications for the Internet of Things (IoT) and Smart Grid will grow significantly in the future due to the quick development of data analytics, connectivity, artificial intelligence (AI), and energy technologies. Key developments and opportunities in both fields are as follows:

1. The Internet of Things

The Internet of Things is growing quickly in homes, cities, and industries. Future developments will probably center on:

a. Growing Use of 5G and Upcoming Technologies:

- IoT devices will be able to operate in real-time with few delays thanks to faster connection and lower latency.
- As more devices connect, communicate, and process data at once, large-scale IoT installations will be feasible.

b. Urban infrastructure and smart cities:

- Smarter public infrastructure will enhance urban living circumstances, such as automated public services and intelligent traffic systems.
- Cities will become more efficient with IoT-based monitoring systems for waste management, energy optimization, and pollution control.

c. Manufacturing and Industry 4.0: • IoT will propel factory automation, with smart devices enhancing production procedures and predictive maintenance averting equipment failures. • Businesses will be able to model and optimize their operations with the help of digital twins, which are virtual copies of actual systems. d. Wearable technology and healthcare:

- Continuous health tracking made possible by remote patient monitoring via IoT-connected gadgets will transform healthcare.
- Real-time health analytics from wearable technology will enhance wellness initiatives, diagnosis, and treatment. e. Intelligent Houses:

• IoT-enabled lighting, security, energy management, and entertainment equipment will be integrated into future smart homes, increasing their level of autonomy.
• AI-powered helpers will manage home automation according to user inclinations and habits. f. Autonomous Vehicles:
• IoT sensors will be essential for communication between vehicles and infrastructure, allowing for safer and more effective autonomous transportation systems.
g. Agriculture and IoT:
• Smart farming will employ IoT to provide real-time data on crop status, weather, and soil health to optimize pesticide, fertilizer, and water use, increasing sustainability and productivity.
2. Applications of Smart Grids
In order to handle issues with energy generation, delivery, and consumption, the smart grid is developing. The scope for the future comprises: a. Renewable Energy Integration:
• By enabling the smooth integration of renewable energy sources like wind and solar, the smart grid will provide effective supply and demand balance.
• IoT technologies will be used to connect and control distributed energy resources (DERs), such as small wind turbines and rooftop solar panels, as part of microgrids.
• b. Advanced Energy Storage: Batteries and other energy storage devices will be essential for storing excess energy from renewable sources and supplying electricity during periods of high demand.
• Electric cars (EVs) will be able to function as mobile energy storage devices by returning power to the grid thanks to vehicle-to-grid (V2G) technology. c. Demand Response and Smart Metering:
• Real-time energy consumption monitoring will be made possible by smart meters, giving users the ability to monitor their usage and optimize energy use. • Demand response systems can be used by utilities to encourage customers to use less energy during peak hours, improving grid stability and cutting expenses.

d. Using AI and Data Analytics to Optimize the Grid:
• AI-powered analytics will support utilities in demand forecasting, power distribution optimization, and outage avoidance.
• IoT-powered predictive maintenance will enable utilities to address problems before they cause interruptions.
f. Decentralized power systems and microgrids:
• Microgrids, which are localized grids that can function independently from the main grid and increase resilience, will become more prevalent in future smart grids.
• With decentralized energy generation, peer-to-peer energy trading systems—where customers may directly purchase and sell excess energy—may proliferate. f. Infrastructure for Charging Electric Vehicles:
• To effectively control load and energy distribution, the increasing usage of electric cars (EVs) will necessitate the development of sophisticated EV charging infrastructure that is connected with smart grids.
• Dynamic pricing for EV charging based on grid demand will optimize electricity use and reduce costs for consumers.
g. Cybersecurity and Grid Protection:
•As the smart grid becomes more complex and interconnected, the risk of cyberattacks will increase. Future grids will incorporate advanced cybersecurity measures to protect against threats and ensure the integrity of the energy system.

The future of IoT and Smart Grid applications promises greater efficiency, sustainability, and convenience across various sectors. These technologies will lead to more connected, intelligent, and resilient systems that improve everything from urban living to energy management, creating a more sustainable and technology-driven future

6. RESULTS AND DISCUSSION

Clinical preparation is improved by blockchain innovation in terms of efficacy and discovery. These data records could be stored on the blockchain as smart contracts composed of digital fingerprints. Uniform authorization processes for access to electronic health information, participant authentication and verification, and extensive network and infrastructure security are just a few advantages of using blockchain technology in the medical field. Turning into Blockchain technology is used for supply chain monitoring and drug liability. This technology makes it possible to keep information on individual patients, which makes it easier to analyze and validate the results of procedures. In addition to improving security and information visibility and transparency, blockchain is used for clinical research, patient monitoring, and medical record preservation. Reduce the time and resources needed for data conversion while maintaining current hospital financial reporting. In an information-driven environment, many problems are solved. Blockchain technology is used to hash individual chunks of patient health records. Patients are also encouraged to provide other parties with the information they require while remaining anonymous thanks to the blockchain system. Numerous instructive signals are expected to lead to preliminary clinical research. Experts focus on these data indicators and conduct studies on a regular basis to examine, evaluate, and calculate productivity ratios in different situations. Future judgments will be made after the data has been analyzed [36–40]. Many researchers, however, are able to alter their conclusions by manipulating the evidence and data they have collected.

Many pharmaceutical companies also want to record results that are useful for their operations. Researchers are therefore using blockchain technology to ensure equity and expedite clinical studies. Facilitates the easy, uneven, and secure recording of clinical trials. The information acquired may provide post-market analysis to improve patient care and maximize financial savings. Open administration of blockchain technology, clear audit trails, resilience, increased privacy, and data security are the foundations of these standards. Because of this, medical practitioners will be able to follow contemporary medical norms, including those pertaining to drug safety. The reasons why blockchain technology should be used in the healthcare industry, as well as the unresolved issues that prevent its widespread use, are crucial to this developing sector.

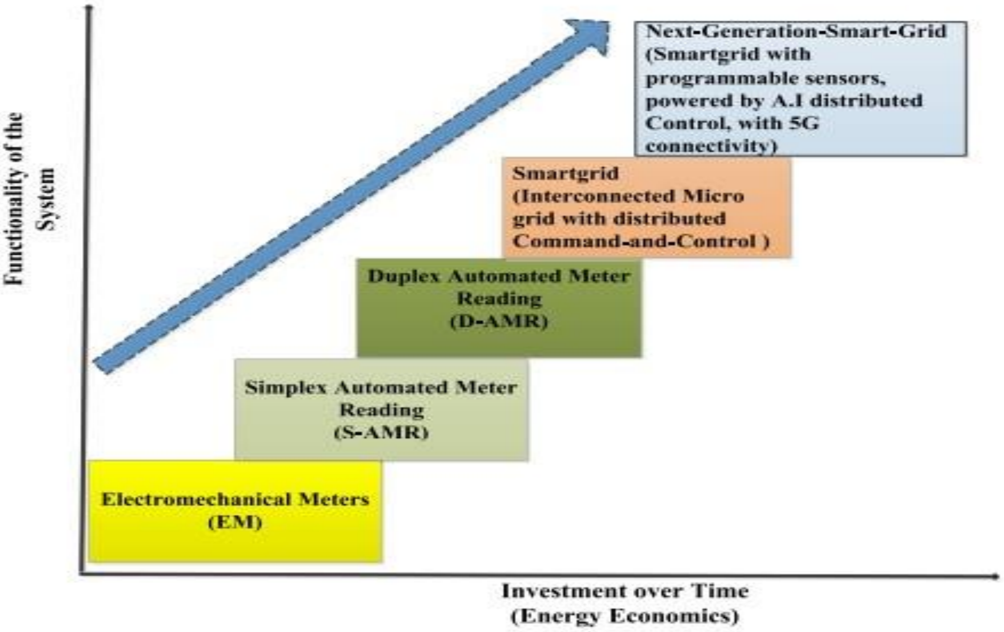

Next-Generation-Smart-Grid (Smartgrid with programmable sensors, powered by A.I distributed Control, with 5G connectivity)
Smartgrid (Interconnected Micro grid with distributed Command-and-Control)
Duplex Automated Meter Reading (D-AMR)
Simplex Automated Meter Reading (S-AMR)
Electromechanical Meters (EM)
Functionality of the System
Investment over Time (Energy Economics)

Figure 4: The evolution from the traditional grid to next generation smart grid

• Rewards

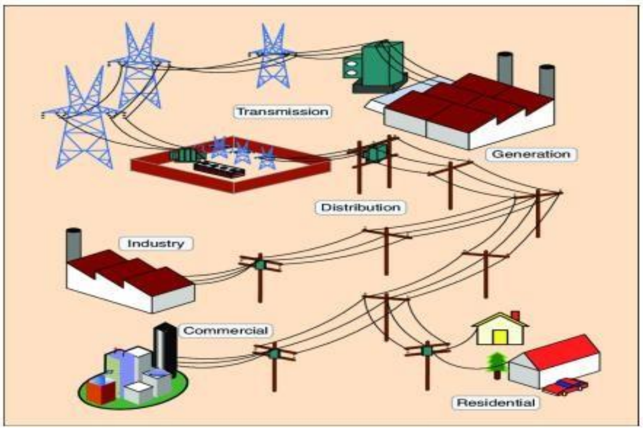


Figure 5: A classical grid

Modern society's efforts to meet needs in a variety of healthcare-related applications have led to the development of blockchain technology. Blockchain technology makes it possible to effectively enhance patient quality without sacrificing system security goals. A review of the studies is carried out in order to look into, categorize, and pinpoint the various benefits and justifications for applying blockchain technology in the healthcare industry. More discussion demonstrates these motivational categories.

Decentralization

Since blockchain distributes medical data over the network rather than at a single security point, its use offers significant advantages for medical data. All stakeholders participating in the medical care industry must have consistent, secure, and immediate access to this information due to the decentralized accountability for data that this biological system considers.

Additionally, this method allows medical data to be managed and transmitted under the guidance of an algorithm that builds a consensus mechanism based on input from trustworthy

network users. A decentralized network has taken the place of the previous healthcare ecosystem, which comprised PHR systems, EHRs, EMRs, teledermatology, telesurgery, and RPMs. By resolving several difficulties, including those pertaining to patient records, the interchangeability of medical data, and the security of healthcare facilities and services, this action has greatly benefited the healthcare industry.

➢ Problems with universal standards and interoperability

There isn't yet a set standard for blockchain accessibility because it is still in its infancy and is evolving quickly. The association would also need to devote more time and energy to integrating blockchain technology in the medical care industry because of the requirement for internationally guaranteed standardization. The standard permit would benefit from a consensus on the type, size, and structure of information that can be kept on the blockchain. If blockchain were built on established standards that businesses could easily accept, adoption would be simpler.

Problems with healthcare organization skills
The idea of a blockchain innovation action plan is not widely known.
Hospitals and other healthcare organizations would need a considerable amount of time to completely switch to blockchain technology from their current RPM, EHR, PHR, and EMR architecture. Blockchain innovation improves the validity and results of clinical preclinical testing. On a blockchain, these papers can be kept as smart contracts within the digital fingerprint. Using blockchain innovations in medical services has several advantages, including member character validation and verification, consistent permission procedures for accessing electronic health data, and comprehensive corporate framework security. Blockchain is utilized to manage pharmaceutical commitments and validate the pharmacy network. This technology helps with the analysis and confirmation of the results of a certain surgery because it may be used to capture information on each unique patient.

Blockchain is used to improve safety, transparency, and information display in addition to clinical trials, patient monitoring, and medical record preservation. It reduces the time and expense of data transformation while maintaining the accuracy of hospital financial accounts. It fixes some issues in the context of data centers. Every block of patient prosperity records will have a hash thanks to the advancement of blockchain technology. Furthermore, the blockchain strategy will encourage patients to provide necessary information to third parties while preserving their privacy. A comprehensive set of educational resources is meant to act as a clinical starting point. The specialists concentrate on these informational indicators and carry out regular experiments to generate evaluations, analyses, and productivity ratios under various conditions. These conclusions are taken into consideration when making additional decisions following the assessment of the data. Blockchain innovation improves clinical preliminary testing's validity and results. These records may be kept on a blockchain as smart contracts within the digital fingerprint. Using blockchain innovations in medical services has several advantages, including secure corporate frameworks, member character validation and verification, and consistent authorization procedures for accessing electronic health data. Drug commitments are tracked and the pharmacy network is validated using blockchain. This technology facilitates the study and confirmation of the results of a certain procedure because it can be used to record unique patient information. Apart from clinical trials, patient monitoring, and medical record retention, blockchain is utilized to improve information display, safety, and transparency. In any case, several analysts can change the results by manipulating the data and verification gathered. Additionally, a lot of pharmaceutical companies want to keep an eye on the outcomes that will help their companies. Therefore, to maintain objectivity and expedite clinical trials, researchers use blockchain technology [40–42]. It will make it easier to document clinical trials in a consistent, secure, and straightforward manner. Patient care may be improved by optimizing efficiency gains through post-market analysis using the collected data [43][44]. These standards are based on the improved privacy and security, open management, transparent auditing trails, robustness, and transparency of data that come with Blockchain technology [45][46]. This allows medical practitioners to adhere to the latest healthcare regulations, including safeguarding pharmaceutical supplies [47].

7. CONCLUSION

Innovative uses in the medical industry are made possible by blockchain's intrinsic decentralization and encryption. It simplifies the production of counterfeit medications for use in combat, encourages the adaptation of health data, improves interoperability across medical service organizations, and fortifies the security of patients' electronic clinical data. Numerous industries that provide medical services could undergo a change thanks to blockchain technology. Facilitating complex arrangements made possible by astute agreements in sectors like medical services is one of blockchain's most significant applications. Expenses will decrease because smart agreements eliminate middlemen from the installment chain.

Blockchain's potential in the healthcare industry is greatly impacted by the ecosystem's adoption of related cutting-edge technology. Clinical studies, health insurance, and system tracking are all included. Hospitals can map out their services using a Blockchain architecture by using device tracking throughout its life cycle. Blockchain technology can be used to extend executives' patient histories, which will speed up healthcare operations and improve information support, particularly during the protection intervention phase. Generally speaking, this invention would greatly enhance and ultimately transform the way medical care administrations are handled, utilized, and organized for both patients and doctors. Blockchain technology has the potential to completely change entire sectors. It could be possible to make the current systems more secure and harder to hack.

The medical services sector is one where information is expanding dramatically. To improve healthcare, technologies like blockchain are required to store data safely, facilitate analysis, and make it easier to track information effectively. The medical services sector has a great opportunity to embrace Blockchain technology and spur innovation. The proposed endeavor entailed applying blockchain technology to the medical domain. This work is limited by the databases we searched. A surge in blockchain-related activities in the healthcare industry has also affected the study's timeline. This study, on the other hand, aims to evaluate the significant amount of blockchain research that has previously been conducted on the healthcare sectors in order to identify any gaps that still exist. Blockchain technology in the healthcare sector has been studied by several academics. In this investigation, bibliometric analysis was concentrated on blockchain and medical care studies.

REFRENCES

1. Zhang, Z., Liu, M., Sun, M., Deng, R., Cheng, P., Niyato, D., ... & Chen, J. (2024). Vulnerability of machine learning approaches applied in iot-based smart grid: A review. IEEE Internet of Things Journal.
2. Ganesh, P. M., Sundaram, B. M., Balachandran, P. K., & Mohammad, G. B. (2024). IntDEM: an intelligent deep optimized energy management system for IoT-enabled smart grid applications. Electrical Engineering, 1-23.
3. Nassereddine, M., & Khang, A. (2024). Applications of Internet of Things (IoT) in smart cities. In Advanced IoT technologies and applications in the industry 4.0 digital economy (pp. 109-136). CRC Press.
4. Hu, Y. (2024). Research on Industry 4.0 smart grid monitoring and energy management based on data mining and Internet of Things technology. Thermal Science and Engineering Progress, 102830.
5. Aoudia, M., Alaraj, M. B., Abu Waraga, O., Mokhamed, T., Abu Talib, M., Bettayeb, M., ... & Ghenai, C. (2024). Toward better blockchain-enabled energy trading between electric vehicles and smart grids in Internet of Things environments: a survey. Frontiers in Energy Research, 12, 1393084.
6. Li, X., Zhao, H., Feng, Y., Li, J., Zhao, Y., & Wang, X. (2024). Research on key technologies of high energy efficiency and low power consumption of new data acquisition equipment of power Internet of Things based on artificial intelligence. International Journal of Thermofluids, 21, 100575.
7. Aouedi, O., Vu, T. H., Sacco, A., Nguyen, D. C., Piamrat, K., Marchetto, G., & Pham, Q. V. (2024). A survey on intelligent Internet of Things: applications, security, privacy, and future directions. IEEE Communications Surveys & Tutorials.
8. Aouedi, O., Vu, T. H., Sacco, A., Nguyen, D. C., Piamrat, K., Marchetto, G., & Pham, Q. V. (2024). A survey on intelligent Internet of Things: applications, security, privacy, and future directions. IEEE Communications Surveys & Tutorials.
9. Yalli, J. S., Hasan, M. H., & Badawi, A. (2024). Internet Of Things (IOT): Origin, Embedded Technologies, Smart Applications and its Growth in the Last Decade. IEEE Access.
10. Liu, P., Wang, J., Ma, K., & Guo, Q. (2024). Joint Cooperative Computation and Communication for Demand-Side NOMA-MEC Systems With Relay-Assisted in Smart Grid Communications. IEEE Internet of Things Journal.
11. Abdi, N., Albaseer, A., & Abdallah, M. (2024). The Role of Deep Learning in Advancing Proactive Cybersecurity Measures for Smart Grid Networks: A Survey. IEEE Internet of Things Journal.
12. Gunduz, M. Z., & Das, R. (2024). Smart Grid Security: An Effective Hybrid CNN-Based Approach for Detecting Energy Theft Using Consumption Patterns. Sensors, 24(4), 1148.
13. Mozny, R., Masek, P., Moltchanov, D., Stusek, M., Mlynek, P., Koucheryavy, Y., & Hosek, J. (2024). Characterizing optimal LPWAN access delay in massive multi-RAT smart grid deployments. Internet of Things, 25, 101001.
14. Bhadani, U. (2024). Smart Grids: A Cyber–Physical Systems Perspective. International Research Journal of Engineering and Technology (IRJET), 11(06), 801.
15. Kushawaha, V., Gupta, G., & Singh, L. (2024). Enhancing Energy Efficiency: Advances in Smart Grid Optimization. International Journal of Innovative Research in Engineering and Management, 11(2), 100-105.
16. Bhadani, U. (2024). Smart Grids: A Cyber–Physical Systems Perspective. International Research Journal of Engineering and Technology (IRJET), 11(06), 801.
17. Olatunde, T. M., Okwandu, A. C., Akande, D. O., & Sikhakhane, Z. Q. (2024). The impact of smart grids on energy efficiency: a comprehensive review. Engineering Science & Technology Journal, 5(4), 1257-1269.
18. Al-Ali, A. R., Gupta, R., Zualkernan, I., & Das, S. K. (2024). Role of IoT technologies in big data management systems: A review and Smart Grid case study. Pervasive and Mobile Computing, 101905.
19. Rostampour, S., Bagheri, N., Ghavami, B., Bendavid, Y., Kumari, S., Martin, H., & Camara, C. (2024). Using a privacy-enhanced authentication process to secure IOT-based smart grid infrastructures. The Journal of Supercomputing, 80(2), 1668-1693.
20. Ezeigweneme, C. A., Nwasike, C. N., Adefemi, A., Adegbite, A. O., & Gidiagba, J. O. (2024). Smart grids in industrial paradigms: a review of progress, benefits, and maintenance implications: analyzing the role of smart grids in predictive maintenance and the integration of renewable energy sources, along with their overall impact on the industri. Engineering Science & Technology Journal, 5(1), 1-20.
21. William, P., Chowdhury, S., Falah, A., Hussain, A., Kumar, R., & Rao, A. L. N. (2024, February). Security Enhancement In Iot Based Smart Grid System Using Cryptographic Techniques. In 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM) (pp. 1-6). IEEE.
22. Arun, M., Gopan, G., Vembu, S., Ozsahin, D. U., Ahmad, H., & Alotaibi, M. F. (2024). Internet of Things and Deep Learning-Enhanced Monitoring for Energy Efficiency in Older Buildings. Case Studies in Thermal Engineering, 104867.
23. Aman, A. H. M., Shaari, N., Bashi, Z. S. A., Iftikhar, S., Bawazeer, S., Osman, S. H., & Hasan, N. S. (2024). A review of residential blockchain internet of things energy systems: Resources, storage and challenges. Energy Reports, 11, 1225-1241.
24. Munoz, O., Ruelas, A., Rosales-Escobedo, P. F., Acuña, A., Suastegui, A., Lara, F., ... & Rocha, A. (2024). Development of an IoT smart energy meter with power quality features for a smart grid architecture. Sustainable Computing: Informatics and Systems, 43, 100990.

25. Kumar, M. P., & Nalini, N. (2024). An efficient chaotic MHT-PUF-based IoT device authentication with QPBFT for smart grid infrastructure. Electrical Engineering, 1-17.
26. Zibaeirad, A., Koleini, F., Bi, S., Hou, T., & Wang, T. (2024). A Comprehensive Survey on the Security of Smart Grid: Challenges, Mitigations, and Future Research Opportunities. arXiv preprint arXiv:2407.07966.
27. Rehman, Z., Tariq, N., Moqurrab, S. A., Yoo, J., & Srivastava, G. (2024). Machine learning and internet of things applications in enterprise architectures: Solutions, challenges, and open issues. Expert Systems, 41(1), e13467.
28. Hoque, K., Hossain, M. B., Das, D., & Roy, P. P. (2024). Integration of IoT in Energy Sector. International Journal of Computer Applications, 975, 8887.
29. Irfan, M., Khan, M. A., & Oligeri, G. (2024, January). Design of Key-dependent S-Box using Chaotic Logistic Map for IoT-Enabled Smart Grid Devices. In 2024 4th International Conference on Smart Grid and Renewable Energy (SGRE) (pp. 1-6). IEEE.
30. Knapp, E. D. (2024). Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Elsevier.
31. Wu, Y., Guo, N., Xu, T., & Li, Q. (2024, July). A privacy calculation method for smart grid power data based on NB IoT. In Third International Conference on Electronic Information Engineering, Big Data, and Computer Technology (EIBDCT 2024) (Vol. 13181, pp. 1464-1469). SPIE.
32. Rajiv, A., Goswami, P. K., Gupta, R., Malik, S., Chauhan, U., & Agarwal, A. (2024). Massive MIMO based beamforming by optical multi-hop communication with energy efficiency for smart grid IoT 5G application. Optical and Quantum Electronics, 56(1), 99.
33. Kiasari, M., Ghaffari, M., & Aly, H. H. (2024). A Comprehensive Review of the Current Status of Smart Grid Technologies for Renewable Energies Integration and Future Trends: The Role of Machine Learning and Energy Storage Systems. Energies, 17(16), 4128.
34. Faheem, M., Kuusniemi, H., Eltahawy, B., Bhutta, M. S., & Raza, B. (2024). A lightweight smart contracts framework for blockchain-based secure communication in smart grid applications. IET Generation, Transmission & Distribution, 18(3), 625-638.
35. Faheem, M., Kuusniemi, H., Eltahawy, B., Bhutta, M. S., & Raza, B. (2024). A lightweight smart contracts framework for blockchain-based secure communication in smart grid applications. IET Generation, Transmission & Distribution, 18(3), 625-638.
36. Anley, M. B., Ekpo, O., & Gedara, T. M. H. (2024). Cybersecurity Assessment of Digital Twin in Smart Grids. In CEUR WORKSHOP PROCEEDINGS (Vol. 3731, pp. 1-10). CEUR-WS. org.
37. Muthulakshmi, S., & Chitra, R. (2024). Interplanetary file system and blockchain for secured smart grid networks. The Journal of Supercomputing, 80(5), 5900-5922.
38. Liu, R., Zhou, N., & Luo, J. (2024, March). The application of power engineering technology in the construction of smart grid. In Second International Conference on Physics, Photonics, and Optical Engineering (ICPPOE 2023) (Vol. 13075, pp. 731-737). SPIE.
39. Wali, M., & Channi, H. K. (2024). Smart Meter Infrastructure for Distributed Renewable Power. In AI Approaches to Smart and Sustainable Power Systems (pp. 81-99). IGI Global.
40. Anusha, M., Kumar, P. B., Akhil, V., Gouthami, M., Chinnaaiah, M. C., & Shaik, S. (2024, April). Internet of Things (IOT) based energy monitoring with ESP 32 and using Thingspeak. In 2024 10th International Conference on Communication and Signal Processing (ICCSP) (pp. 1383-1387). IEEE.
41. Bolgouras, V., Ioannidis, T., Politis, I., Zarras, A., & Xenakis, C. (2024). RETINA: Distributed and secure trust management for smart grid applications and energy trading. Sustainable Energy, Grids and Networks, 38, 101274.
42. Bolgouras, V., Ioannidis, T., Politis, I., Zarras, A., & Xenakis, C. (2024). RETINA: Distributed and secure trust management for smart grid applications and energy trading. Sustainable Energy, Grids and Networks, 38, 101274.
43. Gupta, M., Kumar, R., Sharma, A., & Pai, A. S. (2023, July). Impact of AI on social marketing and its usage in social media: A review analysis. In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE.
44. Baruah, A., Kumar, R., & Gupta, M. (2023, April). Analysis of Traffic Sign Recognition for Automated Transportation Systems Using Neural Networks. In *2023 IEEE 8th International Conference for Convergence in Technology (I2CT)* (pp. 1-5). IEEE.
45. Gupta, A., Kumar, R., & Kumar, Y. (2023). An automatic speech recognition system in Indian and foreign languages: A state-of-the-art review analysis. *Intelligent Decision Technologies*, *17*(2), 505-526.
46. Gupta, M., Kumar, R., & Abraham, A. (2024). Adversarial Network-Based Classification for Alzheimer's Disease Using Multimodal Brain Images: A Critical Analysis. *IEEE Access*.
47. Yadav, A., Kumar, R., & Gupta, M. (2024, March). An analysis of convolutional neural network and conventional machine learning for multiclass brain tumor detection. In *AIP Conference Proceedings* (Vol. 3072, No. 1). AIP Publishing.

A REVIEW ON LONG-DISTANCE OPTICAL FIBER COMMUNICATION

Ramiz Salama, Chadi Altrjman, Sinem Alturjman

Department of Computer Engineering, AI and Robitic Institute, Research Center for AI and IoT,Near East University, Nicosia, Mersin 10 –TurkeyDepartment of Chemical Engineering, Waterloo University, ON N2L 3G1, CanadaArtificial Intelligence, Software, and Information Systems Engineering AI and Robotics Institute,Near East University, Nicosia, Mersin10ramiz.salama@neu.edu.tr, cmfaltrjman@uwaterloo.ca, sinem.alturjman@neu.edu.tr

Abstract—Information can be sent via optical fiber connection, which uses light waves to pass through tiny glass or plastic strands. These fibers are an extremely dependable and effective form of communication since they can send signals over great distanceswith little signal loss. With its fast data transfer rate, optical fiber communication offers a number of benefits, including the abilityto send massive amounts of data quickly. Moreover, optical fibers are resistant to electromagnetic interference, which makes them a good option for sending sensitive data. Optical fibers come in various varieties, such as single-mode fibers that can only transmit one mode of light and multi-mode fibers that can transmit numerous modes of light.Numerous uses for these fibers exist, such as internet connectivity, cable television, and telecommunications. Among other applications, optical fibers are utilized in industrial automation, militarycommunication, and medical imaging. As the need for dependable and fast communication grows, optical fiber use is anticipated to continue expanding in the upcoming years.

Keywords: Optical fiber, Communication, Light wave, Multiplexing, Wavelength, Data rate, Frequency

I.INTRODUCTION

The history of fiber optic communication dates back to the mid-19th century, when the British scientist John Tyndall demonstrated that light could be transmitted through a curved stream of water. However, it wasn't until the 1950s that the first practicalapplication of fiber optic communication was developed. In the 1950s, researchers at Bell Labs developed a method for transmitting light through thin strands of glass, which they called "optical fibers." These fibers were able to transmit signals over longdistances with minimal signal loss, making them a promising alter-native to traditional copper wires for telecommunications. In the 1970s, researchers began to develop ways to manufacture optical fibers on a large scale, and by the 1980s, fiber optic cables had become the standard for long-distance telecommunica-tions. In the 1990s, the development of high-speed internet and the proliferation of the World Wide Web led to a significant increase in the use of fiber optic communica-tion [1-5].Today, fiber optic cables are used in a wide range of applications, including tele-communications, cable television, and internet connectivity. They are also used in medical imaging, military communication, and industrial automation, among other fields. The use of fiber optic communication is expected to continue to grow in the coming years as demand for high-speed and reliable communication increases.Machine learning and AI facilitators started to be part of our daily life and has signif-icant effects towards the rapid developments of the internet of things. One of the leading attempts in this field is the AI learning facilitator, Prof. DUX [6]. It is a novel AI facilitator that aims at personalizing the education process for learners and pro-vide the fastest and best quality of education in numerous fields.

II.EASE OF USEEXTENT OF PAST WORK

The use of optic fiber isn’t limited to communication only. It has proven to be very advantageous to other fields such as themedical industry. Optical fibers are used in a variety of medical applications, including [6-10]:

•Medical imaging: Optical fibers are used in medical imaging techniques, such as endoscopy and laparoscopy, which allow doctors to visualize the inside of the body using a fiber optic camera.
•Surgical instruments: Optical fibers are used in the design of surgical instruments, such as scalpels and forceps, to provide illumination during procedures.
•Phototherapy: Optical fibers are used in phototherapy, a treatment that involves exposing the skin to specific wavelengths of light to improve certain skin conditions, such as acne and psoriasis.
•Dental care: Optical fibers are used in dental care to provide illumination and to cure dental resins used in fillings and crowns.
•Rehabilitation: Optical fibers are used in rehabilitation devices, such as exoskeletons and prosthetics, to provide sensory feedback and improve mobility.
•Overall, the use of optical fibers in the medical industry has greatly improved diagnostic and treatment capabilities, and has led to the development of innovative medical devices and techniques.

III.COMMUNICATIONS ACROSS LONG DISTANCE VIA OPTICAL FIBER

The main material used in optical fiber communication is glass or plastic. These materials are used to create thin strands offiber that are capable of transmitting light signals over long distances [16-20].

•Single-mode fibers are made of pure glass or plastic and are capable of trans-mitting a single mode of light. They are used for long-distance communication and have a small diameter, typically between 8 and 10 micrometers.

•Multi-mode fibers are made of glass or plastic with a higher refractive index and are capable of transmitting multiple modes of light. They have a larger diameter, typically between 50 and 100 micrometers, and are used for shorter-distance communication.The material used can classify the types of optic fiber used in communication: glass fiber or plastic fiber. The main difference between glass and plastic fibers in optical fiber communication is the material used to create the fiber. Glass fibers are made of silica, a type of glass, while plastic fibers are made of polymers, such as polyethylene or polycarbonate.There are a few key differences between glass and plastic fibers in terms of their properties and applications:O Refractive index: The refractive index of a material is a measure of how much it bends light. Glass fibers have a lower refractive index than plas-tic fibers, which means they are less efficient at bending light. This makes them more suitable for transmitting single modes of light over long dis-tances with minimal dispersion. Plastic fibers, on the other hand, have a higher refractive index, which makes them more efficient at bending light. This makes them more suitable for transmitting multiple modes of light over shorter distances.O Diameter: Glass fibers typically have a smaller diameter than plastic fi-bers, which makes them more flexible and easier to install in tight spaces. Plastic fibers, on the other hand, typically have a larger diameter, which makes them more rigid and less flexible.O Transmission loss: Glass fibers typically have lower transmission loss than plastic fibers, which means they are able to transmit signals over longer distances with less signal degradation.O Cost:

Glass fibers are typically more expensive than plastic fibers due to the cost of the raw materials and the manufacturing process.In addition to the fiber itself, there are a number of other materials that are used in optical fiber communication systems, including:O Optical amplifiers: These devices use rare earth elements to amplify the strength of a signal, allowing it to be transmitted over longer distances. There are several types of optical amplifiers, including erbium-doped fi-ber amplifiers (EDFAs), which are used in long-haul communication sys-tems, and semiconductor optical amplifiers (SOAs), which are used in short-haul communication systems.O Modulators: These devices modulate the intensity or phase of a light wave to encode information onto it. There are several types of modula-tors, including intensity modulators, which vary the intensity of the light wave to encode information, and phase modulators, which vary the phase of the light wave to encode information.O Couplers: These devices combine or split optical signals. There are sev-eral types of couplers, including fiber optic couplers, which are used to combine or split signals on a single fiber, and waveguide couplers, which are used to combine or split signalson multiple fibers.O Splitters: These devices divide an incoming optical signal into two or more outputs. There are several types of splitters, including star splitters, which divide an incoming signal into multiple outputs, and tree splitters, which divide an incoming signal into a tree-like structure.O Connectors: These devices allow two optical fibers to be mechanically joined together. There are several types of connectors,including single-fiber connectors, which are used to connect a single fiber to a device, and multi-fiber connectors, which are used to connect multiple fibers to a de-vice.

IV.INSTALLATION

Optical fiber cables are installed by first determining the route that the cable will take, after the cable has been installed, it is tested to ensure that it is functioning properly.Planning and route selection: Before the installation can begin, the route that the cable will take must be planned and chosen. This may involve determining the best path for the cable to follow based on factors such as geography, terrain, and the locations of other infrastructure[21].

•Prepping the cable: Once the route has been determined, the cable is prepared for installation. This may involve stripping the protective coating from the fiber strands and splicing the fibers,together if multiple cables are needed.
•Underground installation: If the cable is being installed underground, a trench must be dug along the planned route. The cable is then placed in the trench and covered with dirt or a protective conduit.
•Aerial installation: If the cable is being installed above ground, it must be attached to poles using special brackets. The cable is then strung between the poles and secured in place.
•Testing: After the cable has been installed, it is tested to ensure that it is functioning properly. This may involve sendinga light signal through the fiber and measuring the signal strength at various points along the cable.
•Connection: Finally, the cable is connected to the necessary equipment, such as repeaters or switches, to complete the installation process. This allows the fiber optic cable to be used for transmitting data and other information[22].Overall, the process of installing optical fiber cables requires careful planning, attention to detail to ensure that the cable is properly installed,and functioning correctly. The optic fiber cables installed may be used differently depending on the industry where it is installed. As seen previously, optic fiber communication is used in a wide range of fields. Here are some explanations on howit is used in each field:
•Telecommunications: In the telecommunications industry, optical fiber cables are used to transmit voice, data, and video signals over long distances. These cables are often used to

connect telephone exchanges, cell phone towers, and other communication infrastructure. For example, an optical fiber cable may be used to transmit a phone call from one city to another, or to connect a cell phone tower to a central office[23].

•Internet service providers: Optical fiber cables are used by internet service providers (ISPs) to provide high-speed internet access to homes and businesses. These cables are often used to connect central offices to neighborhood hubs, and can transmit data at much faster speeds than traditional copper cables. For example, an optical fiber cable may be used to connect a central office to a neighborhood hub, which in turn provides internet access to homes and businesses in that area.

•Cable television: Optical fiber cables are also used in the cable television industry to transmit television signals and other video content. These cables are typically used to connect cable head endsto distribution hubs, and can transmit multiple channels of high-definition video simultaneously. For example, an optical fiber cable may be used to transmit a television program from a cable headend to a distribution hub, which in turn sends the signal to individual homes via coaxial cables[24].

•Medical: Optical fibers are used in the medical field for a variety of purposes, such as illuminating body cavities during surgery and transmitting medical images. For example, an optical fiber may be used to transmit light into a body cavity during surgery, or to transmit an image from an endoscope to a monitor.

•Military: Optical fiber cables are used by the military for secure communication and data transmission, as they are resistant to interference and difficult to tap. For example, an optical fiber cable may be used to transmit sensitive information between military bases or to connect military equipment on the battlefield[25].There are a number of challenges that can be encountered when using optical fiber cables in different industries. Some specific examples of these challenges include:

•Telecommunications: One challenge faced by the telecommunications industry is the cost of installing and maintaining opticalfiber cables. These cables are more expensive to install than traditional copper cables, and can be difficult to repair if damaged. Additionally, telecommunications companies must continually upgrade their networks to keep up with demand for higher speeds and more data.

•Internet service providers: Internet service providers (ISPs) also face the challenge of maintaining and upgrading their networks to keep up with demand for higher speeds and more data. They must also deal with issues such as interference and signal degradation over long distances, as well as the cost of installing and maintaining optical fiber cables.

•Cable television: The cable television industry faces similar challenges in maintaining and upgrading their networks to keepup with demand for higher-quality video and more channels. They must also deal with issues such as signal degradation over long distances and the cost of installing and maintaining optical fiber cables.

•Medical: In the medical field, one challenge faced when using optical fibers is the cost of the equipment and materials needed. Optical fibers and related equipment can be expensive, and replacing damaged fibers or equipment can be costly. Additionally,there are strict regulations and guidelines that must be followed when using optical fibers in medical applications.

•Military: The military faces challenges such as maintaining secure communication and data transmission over long distances, as well as the cost of installing and maintaining optical fiber cables. Additionally, military equipment and infrastructure may be deployed in harsh or remote locations, which can make installation and maintenance more difficult.Overall, the challenges faced when using optical fiber cables in different industries can vary depending on the specific application and industry. However, the high cost and difficulty of installing and maintaining these cables is a common challenge faced bymany industries.

V.RESULTS AND DISCUSSION

There are several advantages of using optical fiber communication, including:

•High data transmission rate: Optical fibers have a high data transmission rate, allowing for the transmission of large amounts of data in a short period of time.
•Immunity to electromagnetic interference: Optical fibers are immune to electromagnetic interference, making them a suitable choice for transmitting sensitive data.
•Low signal loss: Optical fibers have low signal loss, allowing for the trans-mission of signals over long distances with minimal degradation.
•Small size: Optical fibers are thin and flexible, making them easy to install and route through tight spaces.
•Lightweight: Optical fibers are lightweight, making them easy to transport and handle.
•Durability: Optical fibers are resistant to physical damage and can last for many years.
•Versatility: Optical fibers can be used in a variety of applications, including telecommunications, cable television, and internet connectivity. They are al-so used in medical imaging, military communication, and industrial automation, among other fields.
•Energy efficiency: Optical fibers require less power to transmit signals com-pared to traditional copper wire communication systems.
•Cost: In the long term, optical fiber communication systems can be more cost-effective than traditional copper wire systems due to their low maintenanceand replacement costs.
•Security: Optical fibers are difficult to tap or intercept, making them a se-cure option for transmitting sensitive data.
•Ease of installation: Optical fibers are easy to install and route through tight spaces, making them a suitable choice for challenging environments.
•High capacity: Optical fibers have a high capacity for transmitting data, al-lowing for the simultaneous transmission of multiple signals.
•Long lifespan: Optical fibers have a long lifespan and are resistant to physical damage, making them a reliable choice for long-term use.
•Ability to transmit over long distances: Optical fibers are capable of trans-mitting signals over long distances with minimal signal loss, making them a suitable choice for transmitting data over long distances.
•Environmental benefits: Optical fibers donot emit electromagnetic radiation, making them a safer and more environmentally friendly option for communication.Overall, the use of optical fibers for communication offers a number of ad-vantages over traditional copper wire systems, including cost-effectiveness, security, ease of installation, high capacity, long lifespan, high data transmission rates, im-munity tointerference, low signal loss, durability, and the ability to transmit over long distances. Nevertheless, optic fiber communication has some inconveniences or challenges associated with it. Here are some examples of it:

•Initial cost: The initial cost of installing an optical fiber communication system can be high, as it requires specialized equipment and trained personnel.
•Fragility: Optical fibers are thin and fragile, and can be damaged if they are bent or twisted too sharply.
•Splicing: If an optical fiber needs to be repaired or a connection needs to be made, it must be spliced, which requires specialized equipment and trained personnel.

•Limited flexibility: Optical fibers are not as flexible as traditional copper wire systems, and cannot be easily bent or shaped.
•Limited availability: Optical fibers are not as widely available as traditional copper wire systems, and may not be a feasible option in some areas.

•Maintenance: Optical fiber communication systems require regular maintenance to ensure they are functioning properly. This can be time-consuming and may require specialized equipment and trained personnel.
•Distance limitations: While optical fibers are capable of transmitting signals over long distances, they can be affected by dispersion, which can limit the distance over which a signal can be transmitted.
•Signal degradation: Optical fibers can experience signal degradation over time due to factors such as temperature fluctuations, humidity, and physical damage.
•Compatibility issues: Optical fiber communication systems may not be compatible with older equipment or devices that are not equipped to handle optical signals.
•Limited options for connector types: There are fewer options for connector types in optical fiber communication systems compared to traditionalcopper wire systems.

VI.CONCLUSION

Over the past ten years, the fiber optic communications sector has experienced enormous growth and is always evolving. There is still much effort to be done to meet the demand for higher data rates, more advanced switching techniques, and more intelligent network architectures that can dynamically adjust automatically in response to traffic patterns while being economically viable. It is expected that developments in the lab will soon find practical applications, leading to the development of a new generation of fiber optic communications. The advantages of use optical fibers for long-distance communication exceed the disadvantages, notwithstanding these difficulties.Because they require less maintenance and repair over time, optical fiber communication systems may prove to be more affordable in the long run than conventional copper wire systems. They can broadcast many signals simultaneously and have a high data transmission capacity, making them secure due to their difficulty to tap or intercept. Opticalfibers are a dependable option for long-term use since they are resilient to physical harm and have an extended lifespan. Overall, there are numerous benefits to using optical fibers for long-distance communication, such as fast data transfer speeds, immunity to interference, low signal loss, compact size, lightweight, durability, adaptability, and energy efficiency.Although using optical fibers has certain drawbacks, these are surpassed by the advantages, which make them an extremely reliable and efficient choice for long-distance communication.

REFERENCES

[1].Pérez, R. A., Jung, Y., Petropoulos, P., & García, C. V. (2024). Power Over Fiber and Analog Radio Over Fiber Simultaneous Transmission Over Long Distance in Single Mode, Multicore, and Hollow Core Fibers. Laser & Photonics Reviews, 2400157.

[2].Wu, Z., Wu, Z., & Sun, A. (2024). Long distance distributed optical fiber vibration sensing and positioning technology based on loop transmission polarization detection. Measurement, 225, 114029.

[3].Makwana, M., Khant, S., & Patel, A. (2024, March). Advancements in Long-Distance PON Connectivity using WDM and EDFA. In 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 1-6). IEEE.

[4].Kaur, P., Dhawan, D., & Gupta, N. (2024). Investigation of RZ Transmission Using Optical Soliton for Long-Haul Communication. In Latest Trends in Engineering and Technology (pp. 130-135). CRC Press.

[5].Yu, S., Zhao, W., Wang, X., & Zhang, S. (2024, March). Long-distance and high-precision fiber microwave frequency transmission. In Advanced Fiber Laser Conference (AFL2023) (Vol. 13104, pp. 443-447). SPIE.

[6].Devi, P. K., Vidhya, T. H., Selvaraju, M., Balasubramanian, B., Sundar, S., Anvar, J., ... & Hossain, M. A. (2024). High bandwidth profile based on fiber bragg grating dispersion compensation systems for high bit rate optical communications with long distance links. Journal of Optics, 1-11.

[7].Wu, Y., Gao, L., Chai, J., Li, Z., Ma, C., Qiu, F., ... & Zhang, D. (2024). Overview of Health-Monitoring Technology for Long-Distance Transportation Pipeline and Progress in DAS Technology Application. Sensors, 24(2), 413.

[8].Long, Z., Wakamatsu, H., & Iwata, Y. (2024, January). Remote Shape Prediction of Submarine Cables Using Fiber-Optic Distributed Sensors. In 2024 IEEE/SICE International Symposium on System Integration (SII) (pp. 333-338). IEEE.

[9].Rajeev, & Kumar, C. (2024). Effect of various fiber nonlinearities on MADPSK modulated 450× 100 Gb/s ultra-dense WDM system for long haul communication. Journal of Optics, 53(1), 558-573.

[10].Rajeev, & Kumar, C. (2024). Effect of various fiber nonlinearities on MADPSK modulated 450× 100 Gb/s ultra-dense WDM system for long haul communication. Journal of Optics, 53(1), 558-573.

[11].Liu, J., Cai, C., Wang, S., & Wang, J. (2024). Rayleigh length extension in long-distance free-space optical communications based on lens group optimization. Optics Express, 32(10), 16891-16900.

[12].Matsui, T., Sagae, Y., Yamada, Y., Nakajima, K., Matsuo, Y., Inoue, T., ... & Inada, Y. (2024). High Figure–of–Merit Multi–Core Fiber with Standard Cladding Diameter for Long–Haul and Wide–Band Transmission. Journal of Lightwave Technology.

[13].Ali, R. J. A., Jaber, A. T., Ahmed, S. S., & Kadhim, S. A. (2024). Enhancing network performance in a long-haul communication system a wavelength division multiplexing and coherent optical orthogonal frequency division multiplexing approach. Journal of Optics, 1-12.

[14].Sahoo, P. K., & Yadav, A. K. (2024). A comprehensive road map of modern communication through free-space optics. Journal of optical communications, 44(s1), s1497-s1513.

[15].Wu, G., & Tang, M. (2024, May). Theoretical and Experimental Study on the Influence of High Power on Fiber Splice Loss. In 2024 IEEE 6th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC) (Vol. 6, pp. 1175-1179). IEEE.

[16].Adiati, R., & Yani, S. (2024). Comparing the Performance of Optical Communication Links using G. 652 and G. 655 Fiber in Python Packages. Jurnal Pendidikan Fisika dan Teknologi, 10(1), 149-156

17].Hajomer, A. A., Derkach, I., Jain, N., Chin, H. M., Andersen, U. L., & Gehring, T. (2024). Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator. Science Advances, 10(1), eadi9474.

[18].Sakthivel, S., Mansoor Alam, M., Abu Bakar Sajak, A., Mohd Su'ud, M., & Riyaz Belgaum, M. (2024). Review of Compensation and Dispersion Techniques for Fiber Optic Lightpath Networks. International Journal of Computing and Digital Systems, 16(1), 753-767.

[19].Al-Tarawneh, L., Alqatawneh, A., Tahat, A., & Saraereh, O. (2024). Evolution of optical networks: from legacy networks to next-generation networks. Journal of Optical Communications, 44(s1), s955-s970.

[20].Abdulwahid, M. M., Kurnaz, S., Türkben, A. K., Hayal, M. R., Elsayed, E. E., & Juraev, D. A. (2024). Inter-satellite optical wireless communication (Is-OWC) trends: a review, challenges and opportunities. Engineering Applications, 3(1), 1-15.

[21].Singh, P., Kumar, R., Gupta, M., & Al-Turjman, F. (2024). SegEIR-Net: A Robust Histopathology Image Analysis Framework for Accurate Breast Cancer Classification.Current Medical Imaging.

[22].Sharma, H., Kumar, R., & Gupta, M. (2023, March). A Review Paper on Hybrid Cryptographic Algorithms in Cloud Network. In2023 2nd International Conference for Innovation in Technology (INOCON)(pp. 1-5). IEEE.

[23].Larhgotra, A., Kumar, R., & Gupta, M. (2022, November). Traffic monitoring and management system for congestion comtrol using iot and ai. In2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC)(pp. 641-646). IEEE.

[24].Sharma, P., Kumar, R., Gupta, M., & Nayyar, A. (2024). A critical analysis of road network extraction using remote sensing images with deep learning.Spatial Information Research, 1-11.

[25].Kumar, R., Gupta, M., & Sapra, S. R. (2021, October). Speech to text community application using natural language processing. In2021 5th International Conference on Information Systems and Computer Networks (ISCON)(pp. 1-6). IEEE