Smart Grid Networks- Cyber Security Challenges and Blockchain Technology

***Ramiz Salama*[1] and *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 Engineering Dept., AI and Robotics Institute, Near East University, Nicosia, Mersin 10, Turkey*

[3]*Research Center for AI and IoT, Faculty of Engineering, University of Kyrenia, Kyrenia, Mersin 10, Turkey*

ramiz.salama@neu.edu.tr, Fadi.alturjman@neu.edu.tr, Fadi.alturjman@kyrenia.edu.tr

Abstract: The rapid evolution of smart grid networks has brought about transformative changes in the energy sector, revolutionizing power distribution and enabling efficient management of energy resources. However, the proliferation of these advanced networks has also introduced a critical concern - cyber security challenges. As smart grids become increasingly interconnected and reliant on data exchange, they become vulnerable to a range of cyber threats, including unauthorized access, data breaches, and system disruptions. Addressing these challenges is paramount to safeguarding the resilience and security of our energy infrastructure. Fortunately, there is a promising technology that holds potential solutions to the cyber security challenges faced by smart grid networks: blockchain. Originally developed to secure digital transactions in cryptocurrencies like Bitcoin, blockchain technology has evolved into a robust tool with the capacity to enhance security and trust across various domains. By harnessing its core features, such as decentralized consensus, cryptographic algorithms, and an immutable ledger, blockchain can help alleviate critical security concerns in smart grid networks. Additionally, the immutable nature of the blockchain's ledger provides a transparent and auditable record of energy transactions and system operations, enabling efficient monitoring, detection, and response to cyber threats. However, integrating blockchain into smart grid networks comes with its own set of challenges. Scalability, energy efficiency, and interoperability must be meticulously considered to ensure the practicality and effectiveness of the technology. Furthermore, seamless integration of blockchain with existing legacy systems requires careful planning and coordination. This paper looks into the intersection of smart grid networks, cyber security challenges, and blockchain technology. It explores the potential benefits that blockchain can bring to bolster the security and resilience of smart grid networks while shedding light on the technical and operational challenges that must be overcome. Drawing insights from a comprehensive analysis of existing research and real-world case studies, this paper aims to provide valuable guidance and recommendations for stakeholders in the energy industry as they navigate the complexities of adopting blockchain technology as a viable solution to the cyber security challenges faced by smart grid networks.

Keywords: Smart Grid Networks, Cyber Security Challenges, Blockchain Technology, Grid modernization

1. Introduction

A smart grid is an electricity network that employs digital and other cutting-edge technology to monitor and regulate the transmission of electricity from all energy sources to meet the various electrical needs of end users. To operate every component of the system as efficiently as possible, smart grids coordinate the needs and capabilities of all generators, grid operators, end users, and electricity market stakeholders. This maximizes system reliability, resilience, flexibility, and stability while minimizing costs and environmental impacts.

The figure below illustrates the network architecture of a smart grid network:

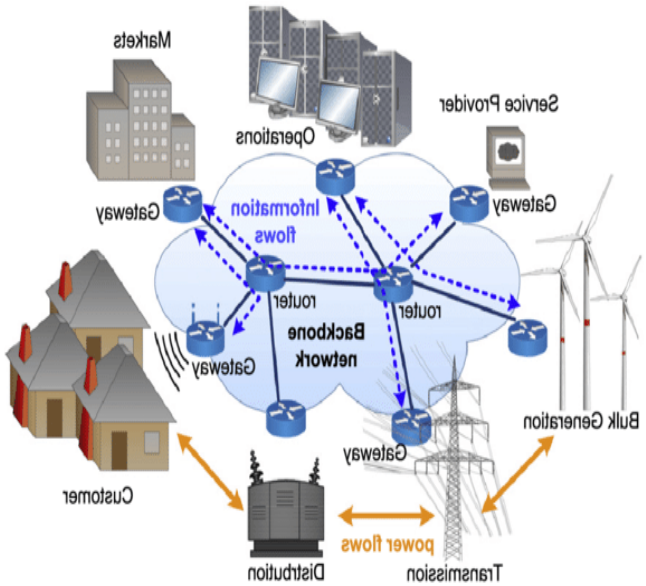

Figure 1. *Smart grid network architecture*

Blockchain technology introduces a decentralized architecture that eliminates single points of failure, effectively thwarting attempts by malicious actors to compromise the entire system. Through the use of advanced cryptographic algorithms, sensitive data within smart grids can be encrypted, ensuring data privacy and integrity.

Here are some key features of a smart grid network:

- Advanced Metering Infrastructure (AMI): Smart meters are deployed to collect detailed information on energy usage, allowing for accurate billing and facilitating demand response programs.
- Distribution Automation: Intelligent devices are installed throughout the distribution system to monitor, control, and automatically respond to changes in electricity flow, reducing outages and improving reliability.
- Renewable Energy Integration: Smart grid networks facilitate the seamless integration of renewable energy sources, such as solar and wind, by enabling real-time monitoring and efficient management of their variable output.
- Energy Management Systems: These systems provide comprehensive monitoring and control capabilities for utilities, allowing them to optimize energy generation, load balancing, and demand response strategies.
- Demand Response Programs: Smart grid networks enable demand response initiatives, where consumers can adjust their electricity usage based on real-time price signals or grid conditions, resulting in reduced peak demand and improved grid stability.
- Grid Resilience and Self-Healing: Through advanced monitoring and automation capabilities, smart grid networks can detect and isolate faults, automatically rerouting power to restore service and minimize disruptions.
- Cybersecurity: Given the increased reliance on digital technologies, smart grid networks incorporate robust cybersecurity measures to protect against cyber threats and ensure the integrity and confidentiality of data.

The ultimate goal of a smart grid network is to create a more efficient, flexible, and sustainable electricity infrastructure that meets the evolving needs of consumers, improves grid reliability, enables the integration of renewable energy sources, and promotes energy conservation.

Machine learning and AI facilitators started to be part of our daily life and has significant 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 [2]. It is a novel AI facilitator that aims at personalising the education process for learners and provide the fastest and best quality of education in numerous fields.

2. Previously published work

Previous researchers have mapped and used essential data on the smart grid to show how popular they have become, as the electricity demand has increased rapidly along with the advancement of the industrial age.

To protect the security of energy trading, the Korean government used blockchain technology with the smart grid. They used the command-line interface (CLI) offered by the blockchain platform known as Multichain to install the blockchain. This system's drawback is that because the simulated system is slow, it cannot be employed in real life.

In the paper, "Energychain: Enabling energy trading for smart homes using blockchains in smart grid ecosystem", the authors created an energy chain to exchange data from smart houses. The power capabilities of various smart homes were used to determine the miner node selection. The information transmitted via the smart grid network was kept in cloud storage. To prevent data tampering in the smart grid network, the miners' responsibility is to authenticate users using local blockchain technology before this process. The system's drawback is that it operated under the assumption that smart meters were reliable sources, which may not always be the case. An algorithm that verifies the accuracy of the data should be applied to the network's smart devices.

In the paper, "Blockchain for smart grid resilience: exchanging distributed energy at speed scale and security", the researchers used blockchain to maintain a secured data exchange within the smart grid network.

They employed smart contracts, which controlled the process of distributing energy without the intervention of a third party. The purpose of smart contracts is to specify the price of exchanged energy as well as the threshold values on which energy is bought or sold. They presented several queries regarding the viability of adopting blockchain technology to secure data sharing. One of the primary concerns was to make sure that blockchain is effective at defending the system against all forms of cyberattacks. The blockchain, which detects any tampering that takes place within the data block, and protects the security of the data block, is the solution to this question. However, this only guarantees security within the smart meter's system.

3. Cyber Security Challenges and Blockchain Technology

A smart grid network refers to an advanced and digitally enabled electricity distribution system that incorporates modern communication, control, and monitoring technologies to enhance the efficiency, reliability, and sustainability of power distribution. Unlike traditional electrical grids, which primarily functioned as one-way systems delivering electricity from power plants to consumers, smart grid networks enable a bidirectional flow of electricity and information. Smart grid networks use various sensors, meters, and automation devices to collect real-time data on energy production, consumption, and grid conditions. This data is then transmitted through communication networks to utility providers, enabling them to monitor and manage the grid more effectively. By analyzing this data, operators can make informed decisions, optimize energy distribution, and promptly respond to disruptions or faults.The choice of materials and methods used in addressing cybersecurity challenges in smart grid networks with blockchain technology may vary depending on specific implementation scenarios. To build a comprehensive and resilient cybersecurity framework within the smart grid network, here are the most common materials used:

- **Blockchain Platforms**:

Different blockchain platforms such as Ethereum, Hyperledger Fabric, or R3 Corda may be used as the underlying technology to implement the blockchain solution for smart grid networks. These platforms provide the necessary infrastructure and tools to build and deploy blockchain-based applications.

- **Cryptographic Algorithms**:

Various cryptographic algorithms are utilized to secure data and transactions in smart grid networks. These algorithms include symmetric encryption, asymmetric encryption, digital signatures, hash functions, and key management protocols.

- **Hardware Security Modules (HSMs)**:

HSMs are dedicated cryptographic devices used to securely store and manage cryptographic keys. They provide hardware-based encryption, key management, and secure execution of cryptographic operations, enhancing the overall security of the blockchain-based smart grid network.

- **Secure Communication Protocols**:

Secure communication protocols, such as Transport Layer Security (TLS) or Secure Shell (SSH), are utilized to ensure secure and encrypted communication between different components of the smart grid network, including blockchain nodes, smart meters, and utility management systems.

- **Firewall and Intrusion Detection/Prevention Systems (IDS/IPS):**

These security appliances are employed to monitor and protect the network infrastructure of the smart grid against unauthorized access and potential cyber threats. Firewalls filter network traffic, while IDS/IPS systems detect and prevent suspicious or malicious activities.

- **Secure Hardware Components**:

Trusted hardware components, such as trusted platform modules (TPMs), secure elements, or secure enclaves, can be utilized to enhance the security of the smart grid network. These components provide secure storage, secure boot, and hardware-based security functionalities. Along with these materials, there are various methods used to further implement blockchain technology:

- **Smart Contract Development**:

Smart contracts are self-executing contracts with the terms and conditions directly written into the code of the blockchain. They enable automation and enforce the rules and agreements between parties involved in smart grid networks. Smart contracts can be developed using programming languages such as Solidity for Ethereum or Chaincode for Hyperledger Fabric.

- **Distributed Ledger Implementation**:

The blockchain's distributed ledger is implemented using consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), or other consensus algorithms. These methods ensure agreement on the state of the network and validate transactions within the smart grid network.

- **Encryption and Data Privacy**:

Cryptographic techniques are employed to encrypt sensitive data within smart grid networks, ensuring data privacy and confidentiality. This involves using encryption algorithms to secure data at rest and during transmission, protecting against unauthorized access or tampering.

- **Access Control and Identity Management**:

Robust access control mechanisms are implemented to manage user authentication and authorization within the blockchain-based smart grid network. This involves assigning unique cryptographic keys or digital identities to participants, ensuring secure and authenticated access to the system.

- **Security Auditing and Monitoring**:

Methods for auditing and monitoring the smart grid network's security posture are implemented to detect and respond to cyber threats. This includes real-time monitoring of network activities, anomaly detection, and incident response procedures.

- **Integration with Existing Systems**:

Methods are employed to integrate the blockchain solution with existing legacy systems and infrastructure within smart grid networks. This involves designing and implementing appropriate APIs and interfaces to enable interoperability and seamless data exchange.

- **Penetration Testing and Vulnerability Assessments**:

Regular penetration testing and vulnerability assessments are conducted to identify potential weaknesses or vulnerabilities in the smart grid network and blockchain implementation. This helps in proactively addressing security gaps and ensuring a robust security posture.

- **Multi-factor Authentication**:

Multi-factor authentication methods, such as using a combination of passwords, biometrics, and one-time password (OTP) tokens, can be implemented to strengthen user authentication and prevent unauthorized access to the blockchain-based smart grid network.

- **Incident Response and Disaster Recovery Planning**:

Well-defined incident response procedures and disaster recovery plans are developed to address and mitigate the impact of security incidents or disruptions in the smart grid network. These plans outline actions to be taken, responsibilities, communication channels, and recovery processes.

- **Security Awareness Training**:

Regular security awareness training programs are conducted for employees and stakeholders involved in the smart grid network. This helps educate them about potential cybersecurity risks, best practices, and how to adhere to security policies and procedures.

- **Regulatory Compliance**:

Compliance with relevant cybersecurity regulations and standards, such as NIST Cybersecurity Framework or ISO/IEC 27001, is ensured to meet industry best practices and protect the smart grid network against potential security breaches.

Here is the architecture of a well-implemented blockchain-based smart grid network:

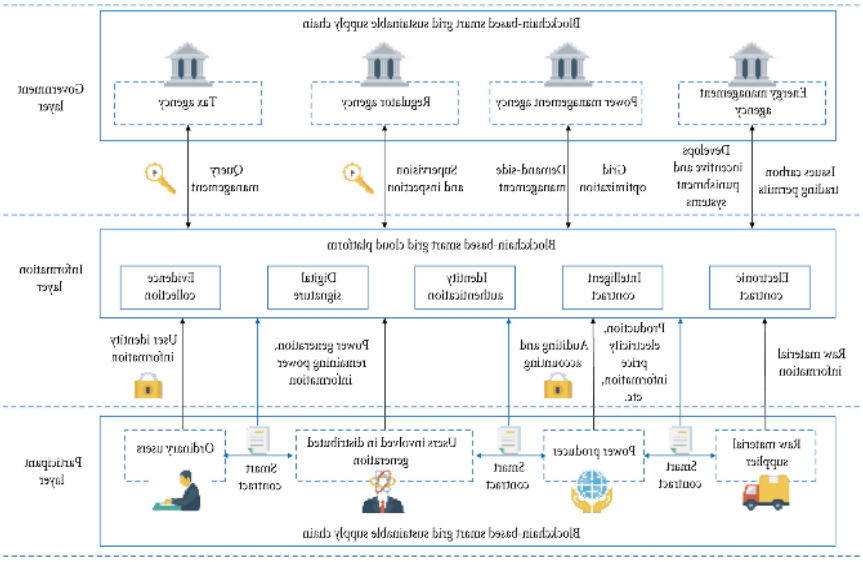

Figure 2. *Blockchain-based Smart Grid Network*

4. Results and discussion

Blockchain technology can play a crucial role in addressing cybersecurity challenges in smart grid networks by providing enhanced security and trust mechanisms.

Here are some ways in which blockchain technology can address these challenges:

- Decentralized Architecture: data is stored and verified across a network of nodes. This eliminates the reliance on a central authority, reducing the risk of single points of failure and making it difficult for malicious actors to compromise the entire system.

- Data Integrity and Immutability: Once data is recorded in a block and added to the chain, it cannot be altered without the consensus of the network participants. This feature prevents unauthorized tampering with critical

data within the smart grid network, maintaining the integrity of energy-related information and ensuring the accuracy of transactions.

- Cryptographic Security: Sensitive data in smart grid networks can be encrypted, providing an additional layer of protection against unauthorized access. Cryptographic techniques such as digital signatures can also be employed to verify the authenticity and integrity of data.

- Access Control and Authentication: Participants in the network can be assigned unique cryptographic keys, allowing for secure and authenticated access to the system. This helps prevent unauthorized entities from accessing or manipulating sensitive data.

- Enhanced Auditability and Transparency: The transparent and auditable nature of blockchain's distributed ledger allows for efficient monitoring, detection, and response to cyber threats. Any changes or transactions recorded on the blockchain can be traced back to their origin, providing a transparent audit trail. This transparency helps in identifying potential security breaches or anomalies in real time.

- Consensus Mechanisms: Blockchain employs consensus mechanisms to validate and agree on the state of the network. Through consensus algorithms such as Proof of Work (PoW) or Proof of Stake (PoS), participants in the network reach a consensus on the validity of transactions and the state of the ledger. This ensures that only verified and legitimate transactions are accepted, mitigating the risk of fraudulent or malicious activities.

While blockchain technology can enhance the security of smart cities, it is not immune to cyber-attacks.

51% Attack: In a blockchain network, the consensus algorithm requires a majority of the nodes to agree on the validity of transactions. If a single entity gains control of more than 50% of the computing power on the network, it can effectively control the blockchain, allowing them to manipulate the transactions. This can result in double-spending attacks, where an attacker can spend the same cryptocurrency twice, or the deletion of transactions from the blockchain. Sybil Attack: In a Sybil attack, an attacker creates multiple fake identities or nodes on the blockchain network, allowing them to control the network. This can enable an attacker to gain access to sensitive data, control smart city systems, or execute fraudulent transactions. Eclipse Attack: In an eclipse attack, an attacker isolates a node on the blockchain network, preventing it from communicating with other nodes, and allowing the attacker to control the node. This can enable an attacker to manipulate the transactions or control the smart city systems connected to the isolated node. Smart Contract Vulnerabilities: Smart contracts are self-executing contracts that run on the blockchain network. However, they can have vulnerabilities that can be exploited by attackers to execute malicious code or steal funds. For example, a smart contract might contain a buffer overflow vulnerability that an attacker can exploit to execute arbitrary code. Distributed Denial of Service (DDoS) Attack: In a DDoS attack, an attacker overwhelms the blockchain network with a large number of requests, causing the network to slow down or crash. This can result in a disruption of smart city services, which can be particularly damaging in critical infrastructure systems. Malware Attacks: Malware can be used to gain unauthorized access to the devices and systems connected to the blockchain network, allowing attackers to steal sensitive information or take control of the systems. For example, an attacker might use malware to gain access to a smart city traffic control system and manipulate traffic signals, causing traffic jams or accidents.

5. Conclusion

In conclusion, smart grid networks' rapid expansion offers the energy sector both amazing possibilities and major cyber security challenges. The risk of illegal access, data breaches, and system outages increases as these networks become more integrated and dependent on data exchange. The security and resilience of smart grid networks can be improved by addressing these vulnerabilities, though, thanks to developing technologies like blockchain. By using a decentralized architecture, cryptographic algorithms, and an immutable ledger of blockchain technology, smart grids can benefit from strengthened security measures. Blockchain's decentralized consensus mechanism eliminates single points of failure, making it difficult for malicious actors to compromise the entire system. Through the use of advanced encryption techniques, sensitive data within smart grids can be securely protected, ensuring data privacy and integrity. Furthermore, the transparent and auditable nature of blockchain's ledger enables efficient monitoring, detection, and response to cyber threats, enhancing the overall cyber resilience of smart grid networks. However, it is important to acknowledge the challenges associated with implementing blockchain technology in smart grid networks. Issues such

as scalability, energy efficiency, and interoperability require careful consideration and innovative solutions. Seamless integration of blockchain with existing legacy systems also demands thoughtful planning and coordination to minimize disruption and maximize effectiveness. Moving forward, stakeholders in the energy industry must collaborate and invest in research and development efforts to fully take advantage of the potential of blockchain technology with addressing the cyber security challenges that occur in smart grid networks. Close cooperation between industry experts, policymakers, and technology providers will be essential to ensure the successful adoption and implementation of blockchain solutions in smart grids. As we navigate the complexities of securing our energy infrastructure in the face of evolving cyber threats, blockchain technology emerges as a powerful tool that can fortify smart grid networks. By embracing this transformative technology, we can create a future where energy systems are resilient, secure, and trustworthy, paving the way for a sustainable and reliable energy landscape.

References

[1]. Salama, R., Al-Turjman, F., Bhatia, S., & Yadav, S. P. (2023, April). Social engineering attack types and prevention techniques-A survey. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 817-820). IEEE.

[2]. Prof. DUX available online: https://dux.aiiot.website/

[3]. Salama, R., Alturjman, S., & Al-Turjman, F. (2023). Internet of Things and AI in Smart Grid Applications. NEU Journal for Artificial Intelligence and Internet of Things, 1(1), 44-58.

[4]. Salama, R., Altrjman, C., & Al-Turjman, F. (2023). A Survey of Machine Learning (ML) in Sustainable Systems. NEU Journal for Artificial Intelligence and Internet of Things, 2(3).

[5]. Salama, R., Altrjman, C., & Al-Turjman, F. (2023). A Survey of Machine Learning Methods for Network Planning. NEU Journal for Artificial Intelligence and Internet of Things, 2(3).

[6]. Salama, R., Altrjman, C., & Al-Turjman, F. (2023). A Survey of the Architectures and Protocols for Wireless Sensor Networks and Wireless Multimedia Sensor Networks. NEU Journal for Artificial Intelligence and Internet of Things, 2(3).

[7]. Al-Turjman, F., Salama, R., & Altrjman, C. (2023). Overview of IoT Solutions for Sustainable Transportation Systems. NEU Journal for Artificial Intelligence and Internet of Things, 2(3).

[8]. Salama, R., Altrjman, C., & Al-Turjman, F. (2023). An overview of the Internet of Things (IoT) and Machine to Machine (M2M) Communications. NEU Journal for Artificial Intelligence and Internet of Things, 2(3).

[9]. Salama, R., Al-Turjman, F., Altrjman, C., & Bordoloi, D. (2023, April). The use of machine learning (ML) in sustainable systems-An Overview. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 821-824). IEEE.

[10]. Al-Turjman, F., & Salama, R. (2021). Cyber security in mobile social networks. In Security in IoT Social Networks (pp. 55-81). Academic Press.

[11]. Al-Turjman, F., & Salama, R. (2021). Security in social networks. In Security in IoT Social Networks (pp. 1-27). Academic Press.

[12]. Salama, R., & Al-Turjman, F. (2022, August). AI in blockchain towards realizing cyber security. In 2022 International Conference on Artificial Intelligence in Everything (AIE) (pp. 471-475). IEEE.

[13]. Al-Turjman, F., & Salama, R. (2020). An overview about the cyberattacks in grid and like systems. Smart Grid in IoT-Enabled Spaces, 233-247.

[14]. Salama, R., Al-Turjman, F., & Culmone, R. (2023, March). AI-Powered Drone to Address Smart City Security Issues. In International Conference on Advanced Information Networking and Applications (pp. 292-300). Cham: Springer International Publishing.

[15]. Salama, R., & Al-Turjman, F. (2023). Cyber-Security Countermeasures and Vulnerabilities to Prevent Social-Engineering Attacks. In Artificial Intelligence of Health-Enabled Spaces (pp. 133-144). CRC Press.

[16]. Salama, R., Al-Turjman, F., Altrjman, C., & Bordoloi, D. (2023, April). The ways in which Artificial Intelligence improves several facets of Cyber Security-A survey. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 825-829). IEEE.

[17]. Salama, R., Al-Turjman, F., Bhatla, S., & Mishra, D. (2023, April). Mobile edge fog, Blockchain Networking and Computing-A survey. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 808-811). IEEE.

[18]. Salama, R., Al-Turjman, F., Chaudhary, P., & Banda, L. (2023, April). Future Communication Technology Using Huge Millimeter Waves—An Overview. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 785-790). IEEE.
[19]. Salama, R., Al-Turjman, F., Aeri, M., & Yadav, S. P. (2023, April). Internet of Intelligent Things (IoT)–An Overview. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 801-805). IEEE.
[20]. Salama, R., Al-Turjman, F., Chaudhary, P., & Yadav, S. P. (2023, April). (Benefits of Internet of Things (IoT) Applications in Health care-An Overview). In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 778-784). IEEE.
[21]. Salama, R., Al-Turjman, F., Altrjman, C., & Gupta, R. (2023, April). Machine Learning In Sustainable Development–An Overview. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 806-807). IEEE.
[22]. Salama, R., Al-Turjman, F., Aeri, M., & Yadav, S. P. (2023, April). Intelligent Hardware Solutions for COVID-19 and Alike Diagnosis-A survey. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 796-800). IEEE.
[23]. Salama, R., Al-Turjman, F., Bhatla, S., & Gautam, D. (2023, April). Network security, trust & privacy in a wiredwireless Environments–An Overview. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 812-816). IEEE.
[24]. Salama, R., Al-Turjman, F., Altrjman, C., Kumar, S., & Chaudhary, P. (2023, April). A Comprehensive Survey of Blockchain-Powered Cybersecurity-A survey. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 774-777). IEEE.
[25]. Salama, R., Al-Turjman, F., Bordoloi, D., & Yadav, S. P. (2023, April). Wireless Sensor Networks and Green Networking for 6G communication-An Overview. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 830-834). IEEE.
[26]. Kumari, M., Gupta, M., & Ved, C. (2021). Blockchain in Pharmaceutical sector. *Applications of blockchain in healthcare*, 199-220.
[27]. Gupta, M., Jain, R., Kumari, M., & Narula, G. (2021). Securing healthcare data by using blockchain. *Applications of blockchain in healthcare*, 93-114.
[28]. 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.
[29]. Kumari, M., Gupta, M., & Ved, C. (2022). Decentralized and Secured Applications of Blockchain in the Biomedical Domain. In *Applications of Blockchain and Big IoT Systems* (pp. 267-282). Apple Academic Press.
[30]. Kumar, P., Gupta, M., & Kumar, R. (2023, July). Improved Cloud Storage System Using IPFS for Decentralised Data Storage. In *2023 International Conference on Data Science and Network Security (ICDSNS)* (pp. 01-06). IEEE.
[31]. Kumar, D., & Gupta, M. (2018). Implementation of firewall & intrusion detection system using pfSense to enhance network security. *International Journal of Electrical Electronics & Computer Science Engineering*, *1*, 2454-1222.
[32]. Gupta, M., Yadav, R., & Tanwar, G. (2016, March). Insider and flooding attack in cloud: A discussion. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 530-535). IEEE.
[33]. Gupta, D., Kaur, H., & Kumar, R. (2016). Detection of sink hole attack in wireless sensor network using advanced secure AODV routing protocol. *International Journal of Computer Applications*, *156*(11).
[34]. Madhu, D. R. K., & Kaur, S. Secure Channel and Watch-Dog based technique for Isolation of Wormhole Attack in MANETs.