Blockchain Technology-Security and Privacy in Mobile Cloud Computing

***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: Mobile cloud computing is a technology that allows users to access cloud services using mobile devices. It has become increasingly popular due to its convenience and flexibility. However, security and privacy are major concerns when it comes to mobile cloud computing. Blockchain technology has been proposed as a solution to these issues. Blockchain is a decentralized and distributed ledger that can be used to store data securely and transparently. It can also be used to provide secure access control and identity management. Blockchain technology holds the potential to significantly increase data privacy and security while boosting accuracy and integrity in cloud data. It can also be used to provide secure data sharing between different organizations. This paper will help to review blockchain technology and its fundamental principles, highlighting its decentralized architecture, immutability, and cryptographic techniques. We will discuss how blockchain can address the security and privacy gaps in mobile cloud computing. Specifically, it explores the potential of blockchain for secure data storage, access control, trust management, and authentication in mobile cloud environments.

Keywords: Mobile Cloud Computing, Blockchain Technology, Cloud Computing Security, Data Privacy

1. Introduction

Mobile cloud computing (MCC) is a method of delivering mobile apps using cloud technology. Complex mobile apps today carry out tasks including authentication, location-aware features, and providing users with customized communication and content. As a result, they need a lot of computational resources, including processing power, memory, and data storage. By utilizing the power of cloud infrastructure, mobile cloud computing relieves mobile devices of some of their burden.

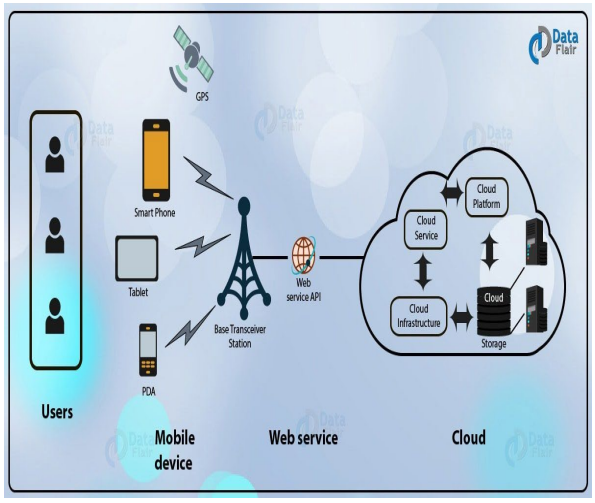

Figure 1. *Mobile cloud computing architecture*

As pictured in the figure above, Mobile Cloud Computing architecture is intended to give mobile users, network operators, and cloud computing provider's extensive computational resources where data processing and storage take place outside of the mobile devices.

Mobile cloud computing presents many advantages such as:

- Increased Storage Capacity: Mobile devices typically have limited storage capacity. With mobile cloud computing, users can offload their data storage to the cloud, providing unlimited virtual storage space for their files, documents, photos, and videos.

- Enhanced Accessibility: Mobile cloud computing allows users to access their data and applications from anywhere with an internet connection. This level of accessibility ensures that users can work on their files and access their resources on multiple devices, enabling seamless productivity and collaboration.

- Cost Efficiency: By using cloud services, users can reduce hardware and infrastructure costs. They no longer need to rely on expensive hardware upgrades or maintenance since the cloud provider takes care of the underlying infrastructure. Users simply pay for cloud services on a subscription basis, allowing them to scale resources up or down as needed, resulting in cost savings and operational flexibility.

- Seamless Synchronization: Mobile cloud computing enables synchronization of data across multiple devices. Users can start a task on one device and seamlessly continue it on another without the need for manual data transfer. This synchronization ensures consistency and convenience, enhancing productivity and user experience.

- Enhanced Computing Power: Mobile devices often have limited processing power and memory capacity. By offloading computational tasks to the cloud, mobile cloud computing allows users to leverage the powerful computing resources available in the cloud. This enables resource-intensive applications, such as complex calculations or high-definition video rendering, to be executed efficiently on mobile devices.

- Improved Collaboration: Mobile cloud computing facilitates seamless collaboration among users. Multiple individuals can access and edit documents simultaneously, share files, and collaborate on projects in real time. This level of collaboration enhances teamwork, communication, and productivity in both personal and professional settings.

- Data Backup and Recovery: Mobile cloud computing provides automatic data backup and recovery mechanisms. In the event of device loss, damage, or failure, users can easily retrieve their data from the cloud, ensuring data integrity and minimizing the risk of permanent data loss.

- Scalability and Flexibility: Mobile cloud computing allows users to scale their resources based on their needs. Whether it's expanding storage capacity or increasing computing power, cloud services offer scalability and flexibility to accommodate changing requirements, ensuring optimal performance and resource utilization.

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**

Research efforts focusing on integrating blockchain technology for enhancing security and privacy in mobile cloud computing have been gaining momentum in recent years. While the field is still evolving, there have been major efforts to investigate and suggest solutions that use blockchain in the context of mobile cloud security and privacy.

Here are some key areas that have received attention in previous studies:

- Secure Data Sharing and Access Control: Researchers have delved into using blockchain to ensure secure data sharing and access control in mobile cloud computing. By leveraging blockchain's capabilities, access control mechanisms can be implemented, allowing users to define and enforce precise permissions for data access. This ensures that only authorized individuals can retrieve and modify data stored in the cloud.

- Privacy-Preserving Solutions: Several studies have explored privacy-preserving techniques using blockchain in mobile cloud computing. These solutions aim to protect sensitive data's confidentiality during storage and processing while still enabling secure computations and data sharing among multiple parties.

- Identity Management and Authentication: Blockchain has been examined as a means to enhance identity management and authentication in mobile cloud computing. Decentralized identity systems built on blockchain empower users with control over their digital identities. This improves the authentication process and reduces the risk of identity theft and unauthorized access.

- Secure Data Storage and Auditing: Proposed blockchain-based solutions seek to enhance the security and integrity of data storage in mobile cloud environments. By storing data on the blockchain, the tamper-resistant nature of the ledger ensures data integrity. Additionally, the distributed nature of blockchain mitigates the risks associated with data loss or unauthorized access.

- Trust and Reputation Systems: Blockchain technology has been applied to establish trust and reputation systems in mobile cloud computing. Recording and verifying transactions and interactions on the blockchain build trust among users and service providers, enabling more secure and reliable collaboration within the mobile cloud.

- Consensus Mechanisms for Security: Researchers have explored different consensus mechanisms and algorithms within the blockchain to enhance the security of mobile cloud computing. These consensus protocols ensure the immutability and integrity of data stored on the blockchain, adding an extra layer of security to the mobile cloud ecosystem.

3. Blockchain Technology, "Security and Privacy"

3.1. In Mobile Cloud Computing

Security and privacy concerns in mobile cloud computing are significant due to the inherent vulnerabilities and risks involved in the interaction between mobile devices and cloud services.

Let’s dive deeper into those security and privacy concerns that come along with the use of the Internet:

- Data Breaches: Mobile cloud computing involves the transmission and storage of sensitive data over the network and on cloud servers. If proper security measures are not in place, there is a risk of data breaches and unauthorized access to confidential information.

- Unauthorized Access: Mobile devices are susceptible to theft, loss, or unauthorized physical access. If proper security measures, such as strong authentication and encryption, are not implemented, unauthorized individuals may gain access to the device or cloud accounts, potentially compromising data and privacy.

- Insecure Communication Channels: Communication channels between mobile devices and cloud services may be vulnerable to interception, eavesdropping, and man-in-the-middle attacks. Without proper encryption and secure communication protocols, sensitive information can be exposed during transmission.

- Cloud Service Provider Security: Trust in the cloud service provider is crucial for mobile cloud computing. Users must rely on the security practices and measures implemented by the provider to protect their data. Concerns include the provider's data handling practices, adherence to security standards, and vulnerability to insider threats.

- Data Privacy: Mobile cloud computing involves the collection, storage, and processing of personal data. Users are concerned about the privacy of their information, including the use, sharing, and potential misuse of their data by mobile apps and cloud services.

- Compliance and Legal Issues: Mobile cloud computing may involve compliance with data protection regulations, industry standards, and legal requirements. Failure to comply with these regulations can result in legal and financial consequences, especially when dealing with sensitive or personally identifiable information.

- Device and Application Security: Mobile devices are susceptible to malware, viruses, and unauthorized access through compromised applications. Malicious apps can access sensitive data, track user behavior, or exploit vulnerabilities in the device's operating system.

- Data Loss and Data Recovery: Mobile devices can be lost, stolen, or damaged, leading to potential data loss. If proper backup and recovery mechanisms are not in place, users may permanently lose their data, compromising both confidentiality and availability.

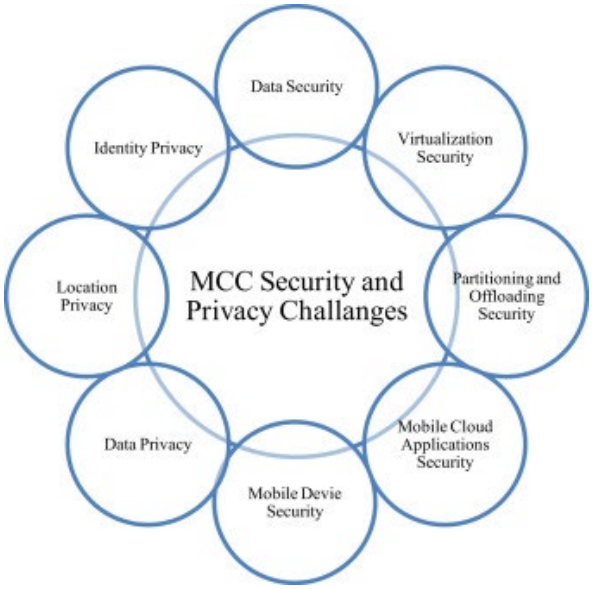

Figure 2. *Mobile Cloud Computing Security and Privacy Challenges*

Blockchain technology is a promising solution because of its unique characteristics that make it suitable for managing sensitive data and ensuring secure transactions.

A blockchain is a database that is distributed across a network of computers, rather than being stored in a central location. Each computer in the network, or "node," has a copy of the database, which is constantly updated and synchronized with the other nodes.
This means that there is no single point of failure or control, and the data is more resilient to hacking, data loss, or other types of attacks.

Blockchain technology can contribute to addressing security and privacy concerns in mobile cloud computing through the following mechanisms:

- Data Integrity and Immutable Audit Trail: Blockchain provides an immutable and tamper-resistant distributed ledger where transactions and data records can be securely stored. By leveraging blockchain, mobile cloud computing can ensure the integrity of data, preventing unauthorized modifications or tampering. This feature enhances data trustworthiness and reduces the risk of data breaches.

- Decentralization and Trustless Environment: Blockchain's decentralized nature eliminates the need for a central authority, reducing the risk of a single point of failure or malicious manipulation. In mobile cloud computing, blockchain can establish a trustless environment where users can interact directly, minimizing the need to rely solely on cloud service providers for security and privacy.

- Access Control and User Authentication: Blockchain-based identity management systems can provide secure and decentralized access control mechanisms. Users can have control over their digital identities and authenticate themselves securely, reducing the risk of unauthorized access to cloud resources and enhancing overall system security.

- Secure Data Sharing and Consent Management: Blockchain can enable secure and auditable data sharing among multiple parties while maintaining data privacy. Smart contracts on the blockchain can enforce data-sharing policies and consent management, ensuring that data is only accessed and used according to predefined rules and permissions.

- Transparent and Auditable Transactions: Blockchain's transparency allows for auditability and accountability in mobile cloud computing. By recording transactions and data access on the blockchain, it becomes possible to trace and verify the usage of data, detect unauthorized access attempts, and ensure compliance with regulations and privacy requirements.
-
- Enhanced Trust and Privacy-Preserving Solutions: Blockchain can facilitate the development of privacy-preserving solutions in mobile cloud computing. Techniques such as zero-knowledge proofs and secure multi-party computation can be integrated with blockchain to enable secure computations and data processing without exposing sensitive information.

- Data Ownership and Consent Tracking: Blockchain's decentralized nature enables users to have better control over their data ownership and consent management. Users can track and revoke access to their data, giving them more control over how their information is shared and used in the mobile cloud environment.

4. Results and discussion

Before the integration of blockchain technology, security and privacy in mobile cloud computing were addressed using various traditional approaches. s
Here are some common methods:

- Encryption: Data encryption techniques, such as symmetric and asymmetric encryption algorithms, were used to protect data during transmission and storage in mobile cloud environments. Encryption ensures that data is unreadable to unauthorized individuals even if it is intercepted or compromised.

- Access Control: Access control mechanisms were implemented to regulate user access to cloud resources and data. This involved authentication processes, user roles and permissions, and fine-grained access control policies to ensure that only authorized users could access specific resources.

- Secure Communication Protocols: Secure communication protocols, such as SSL/TLS, were employed to establish secure connections between mobile devices and cloud servers. These protocols encrypt the communication channels, preventing eavesdropping or tampering with data during transmission.

- Firewalls and Intrusion Detection/Prevention Systems: Firewalls and intrusion detection/prevention systems were deployed to monitor network traffic, detect malicious activities, and prevent unauthorized access to mobile cloud environments. These security measures help protect against common attacks, such as network intrusion and denial-of-service attacks.

- Data Backup and Disaster Recovery: Regular data backup and disaster recovery strategies were implemented to ensure that data could be restored in the event of data loss or system failures. These measures involved storing redundant copies of data in geographically dispersed locations and implementing backup and recovery processes.

- Privacy Policies and Consent Management: Privacy policies and consent management frameworks were established to govern the collection, use, and sharing of user data in mobile cloud environments. Organizations were required to obtain user consent and provide transparency regarding how data is handled, ensuring compliance with privacy regulations.

- Security Audits and Compliance: Regular security audits were conducted to assess the effectiveness of security controls and identify potential vulnerabilities or weaknesses in mobile cloud systems. Compliance with industry standards and regulations, such as ISO 27001 or HIPAA, helped ensure security and privacy requirements were met.

While these traditional approaches offered some level of security and privacy protection, they often relied on centralized authorities and were susceptible to single points of failure or vulnerabilities. Blockchain technology provides additional benefits, such as decentralization, immutability, and transparency, that can further enhance security and privacy in mobile cloud computing.

Integrating blockchain technology into mobile cloud computing has brought several benefits. Here are some of the advantages:

- Enhanced Security: Blockchain provides a decentralized and tamper-resistant ledger, ensuring the security and integrity of data stored and exchanged within the mobile cloud. Its cryptographic algorithms and consensus mechanisms make it difficult for malicious actors to compromise the system or tamper with stored data.

- Data Integrity and Immutability: Blockchain's immutable nature ensures that once data is recorded on the blockchain, it cannot be altered or deleted without consensus from the network participants. This feature is particularly valuable in mobile cloud computing, where data integrity is crucial for maintaining trust in the system.

- Decentralization and Trustless Environment: By using blockchain, mobile cloud computing can move away from centralized authorities and create a trustless environment. Participants can interact directly, eliminating the need for intermediaries and reducing reliance on single points of failure. This decentralization enhances system resilience and mitigates the risk of unauthorized manipulation or control.

- Improved Privacy and Data Ownership: Blockchain can provide solutions for privacy and data ownership concerns in mobile cloud computing. Through techniques like zero-knowledge proofs and encryption, sensitive data can be securely stored and shared while preserving user privacy. Users have more control over their data, granting or revoking access as needed.

- Smart Contract Automation: Smart contracts, programmable self-executing contracts on the blockchain, can automate processes and enforce predefined rules in mobile cloud computing. This automation reduces the need for intermediaries and manual interventions, streamlining operations and reducing costs.

- Efficient and Trustworthy Transactions: Blockchain technology enables faster and more efficient transactions by eliminating the need for intermediaries, reducing paperwork, and streamlining verification processes. Additionally, the trustworthiness of transactions is enhanced, as each transaction is recorded on the blockchain and verified by the consensus of network participants.

- Improved Collaboration and Interoperability: Blockchain facilitates secure and transparent collaboration among different stakeholders in the mobile cloud ecosystem. It allows for interoperability between diverse systems and applications, enabling seamless integration and data exchange between different platforms and organizations.

5. Conclusion

In conclusion, the combination of Mobile Cloud Computing (MCC), Security, Privacy, and Blockchain Technology offers a promising solution to address the concerns surrounding data protection and privacy in mobile cloud

environments. As mobile devices and cloud computing become increasingly popular, it's crucial to ensure that sensitive information remains confidential, integral, and accessible. Furthermore, the collection and use of personal data by mobile apps have amplified the need for strong privacy protection. Blockchain technology, with its decentralized and unchangeable nature, can help improve security and privacy in mobile cloud computing. By using blockchain's distributed ledger and advanced security techniques, we can establish a trustworthy environment for secure data storage, access control, trust management, and user authentication. Smart contracts also play a role in automating security and privacy rules, making processes more transparent and accountable. However, we must acknowledge that integrating blockchain into mobile cloud systems comes with challenges. We need to address issues related to scalability, performance, and how blockchain fits into existing systems. Researchers and industry experts are actively working to overcome these limitations and optimize the use of blockchain in mobile cloud environments. Looking ahead, it's important to continue exploring innovative approaches that balance security, privacy, and usability in mobile cloud computing. Collaboration among researchers, professionals, and policymakers is key to establishing standardized frameworks, best practices, and regulations that protect data and privacy. By using the potential of blockchain technology, the security and privacy of mobile cloud computing can be transformed, creating a more trustworthy and resilient ecosystem. With careful consideration of the technical challenges, ongoing improvements in blockchain, and collaboration among stakeholders, we can envision a future where users confidently use mobile cloud services while safeguarding their security and privacy.

References

[1]. 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.

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

[3]. 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.

[4]. 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.

[5]. 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.

[6]. Salama, R., Altrjman, C., & Al-Turjman, F. (2023). Smart Grid Applications and Blockchain Technology in the AI Era. NEU Journal for Artificial Intelligence and Internet of Things, 1(1), 59-63.

[7]. 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.

[8]. 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).

[9]. 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).

[10]. 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).

[11]. 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).

[12]. 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.

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

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

[15]. 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.

[16]. Al-Turjman, F., & Salama, R. (2020). An overview about the cyberattacks in grid and like systems. Smart Grid in IoT-Enabled Spaces, 233-247.
[17]. 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.
[18]. 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.
[19]. 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.
[20]. 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.
[21]. 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.
[22]. 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.
[23]. 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.
[24]. 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.
[25]. 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).
[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.
[35]. Gupta, M., & Singla, N. (2019). Evolution of cloud in big data with hadoop on docker platform. In *Web services: Concepts, methodologies, tools, and applications* (pp. 1601-1622). IGI Global.
[36]. 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.
[37]. Gupta, M. (2023). A novel scheme to manage the e-healthcare system using cloud computing and the internet of things. In *Computational Intelligence in Healthcare* (pp. 81-97). CRC Press.