Selective Idea of Decentralized Multi-Layered Blockchain Security Framework for IoT Devices

Ahmad Anwar Zainuddin[1], Amir 'Aatieff Amir Hussin[1], Nik Nor Muhammad Saifudin[1], Sultan Ariffin Kamal[2], Nurul Hanis Mohd Dhuzuki[1], Muhammad Haqim Hazhar[2], Muhammad Iman Hakeem M.D Khairi[2], Muhammad Syahmi Noorhisham[2]

[1] Department of Computer Science, Kulliyyah of ICT, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[2] Department of Information Technology, Kulliyyah of ICT, International Islamic University Malaysia, Kuala Lumpur, Malaysia

***Abstract*— The limited memory and processing power of individual devices is one of the main issues facing the IoT ecosystem. Environmental security needs to be authenticated for preserving user confidence and protecting sensitive data. In this study, selective overview of Blockchain-Based Security Architecture has been proposed to find the solution in environment security. Delving into understanding the fundamentals of blockchain technology, including its decentralized nature, cryptographic principles, consensus mechanisms, and smart contracts. By leveraging blockchain-based security mechanisms, the proposed architecture contributes to enhancing environmental security within the IoT ecosystem. It ensures the integrity and confidentiality of sensitive data related to environmental monitoring, resource management, and sustainability initiatives.**

***Index Terms*— IoT, Blockchain, Security**

I. Introduction

The present Internet-of-Things landscape has seen a rapid growth of networked gadgets that have completely changed the way people engage with technology. These networked gadgets, which range from wearable fitness trackers to smart thermostats, provide previously unheard-of efficiency and ease. But there are also a lot of obstacles associated with this exponential rise in IoT devices, especially when it comes to security and privacy. With billions of devices producing data every second, there is a high risk of security lapses and invasions of privacy [1].

The limited memory and processing power of individual devices is one of the main issues facing the Internet of Things ecosystem. Many IoT devices, in contrast to conventional computers or servers, run on limited hardware, frequently with limited processing and memory capacity [2]. This restriction presents a significant obstacle to putting strong security measures in place. For instance, IoT devices with low capabilities may find it difficult to process encryption algorithms that guarantee data secrecy. Furthermore, if authentication and authorization overhead is not adequately controlled, it may put a strain on these devices' capabilities and result in vulnerabilities or performance problems [3].

Notwithstanding these difficulties, preserving user confidence and protecting sensitive data depend heavily on IoT environment security. In this endeavor, authentication and authorization techniques are essential since they provide the basis of secure communication between connected devices [4]. Robust authentication systems, such biometric recognition or two-factor authentication, aid in confirming the identification of devices and stop unwanted access. Such as wise, strong authorization protocols limit what each device can do on the network, reducing the possibility of malicious activity. A proactive approach to risk management and a focus on security measures can help stakeholders reduce the security and privacy issues that come with the expanding IoT ecosystem [5].

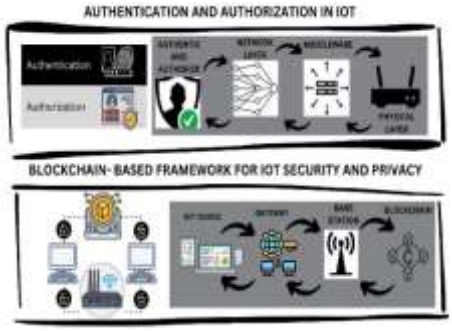

Figure 1:Aunthentication and Authorization in IOT, Blockchain-Based Frameworks for IoT Security and Privacy

Figure 1 shows that ttraditional access control methods, such as Public Key Infrastructure (PKI) and central authorities, have limitations such as increased work and delays. To tackle these problems, alternative approaches have been suggested, such as using blockchain technology. It is proposed a blockchain-based access management system for the IoT, using a Proof-of-Concept consensus algorithm instead of a centralized control server. This method also solves issues with access rights delegation by utilizing Ethereum blockchain technology for

DOI:http://doi.org/10.24086/cocos2024/paper.1491

entity identification. The research proposes a blockchain structure with layers, intersections, and self-organization to confirm IoT entities and analyses security performance and model efficiency based on storage efficiency, response time, and verification. Our publication emphasizes the challenges of data authentication security and privacy in IoT and suggests using blockchain to eliminate the need for a central server and address problems such as device impersonation, fraudulent authentication, and unreliable data exchange. The suggested blockchain-based architecture aims to overcome the problem of a single point of failure.

Many individuals in blockchain technology have been actively engaged in developing solutions to tackle challenges such as data privacy, scalability, and the absence of standardized designs. Professionals across various projects and initiatives are dedicated to advancing the capabilities of blockchain systems. Exploring recent publications, conference papers, and industry reports can shed light on the collective efforts and contributions made by experts working towards enhancing blockchain technology. Additionally, examining the teams associated with leading blockchain projects and organizations involved in research can provide valuable insights into the collaborative work addressing these critical issues. They have introduced the Lightweight Scalable Blockchain (LSB) as part of their expansion, with the goal of enhancing the security and privacy of IoT devices. Furthermore, they've developed sophisticated consensus algorithms like Proof of Block and Trade (PoBT) to accelerate ledger distribution and validation, while simultaneously decreasing computation time. The Lightweight Scalable Blockchain (LSB) aims to improve security and privacy in IoT devices by utilizing a blockchain framework powered by devices with strong computational abilities. It introduces a new consensus algorithm called Proof of Block and Trade (PoBT) to tackle the challenges of combining blockchain technology with scalable IoT networks. The goal is to decrease the time required for blocking and trade validation.

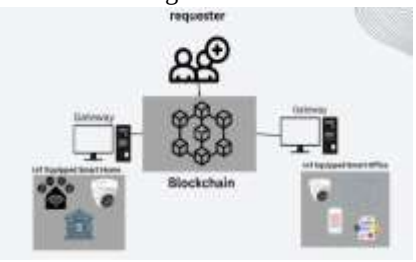

Figure 2: Permissioned Blockchain in IoT

Figure 2 shows the usage of permissioned blockchain, notably Hyperledger Fabric (HLF), in IoT applications is also explained. HLF's distributed ledger technology fosters flexibility, scalability, and confidentiality by offering a reliable environment free from reliance on a central authority. For managing IoT big data, an authorization framework based on HLF is presented to improve consensus algorithms and address security and trust issues.

Figure 3: Layer-Based IoT Blockchain

Figure 3 shows the use of multi-tier structures for specific purposes, such as secure communication in smart cities and healthcare. They combine blockchain technology and Software Defined Networking (SDN) in hybrid network setups to maximize efficiency. By incorporating mobile agents to perform necessary functions, the multi-level blockchain framework improves data security and privacy in IoT applications. This also introduces a multi-layer security architecture for IoT devices connected to multi-hop cellular networks. This architecture uses machine learning and intelligent clustering techniques with Evolutionary Computation (EC) and Swarm Intelligence (SI) algorithms. By combining local authentication services with a globally distributed blockchain-based framework, the proposed network model aims to provide a reliable and trustworthy security mechanism while ensuring increased privacy, scalability, and flexibility anywhere in the paper.

The first section outlines the introduction of the IoT.Section 2 contains brief information about the Methodology.Section 3 is the Selective idea of multilayer blockchain-based security, Section 4 is the Strategy of integration of blockchain and IoT in smart devices and Section 5 concludes the overall case study.

II. METHODOLOGY

In this work, several papers have been studied to initiate the establishment of an IoT Multi-Layer Blockchain-Based Security System which involves a systematic approach to identify, analyze, and address security challenges within IoT networks. By leveraging techniques such as Simulated Annealing and Genetic Algorithm, along with the creation of device groupings and the designation of local security leaders, organizations can enhance the security posture of their IoT infrastructure. The implementation of private blockchains for each device group provides a decentralized and secure framework, enabling encrypted and authenticated communication within and between groups. Security protocols tailored to the specific needs of each group contribute to a comprehensive defense against unauthorized access, data integrity issues, and other vulnerabilities. Regular monitoring, updates, and audits are essential for maintaining the effectiveness of the security system over time. Additionally, educating and training stakeholders, along with staying informed about emerging technologies, ensures a proactive and adaptive approach to cybersecurity. In adopting this multi-layered security strategy, organizations can establish a resilient IoT environment that not only mitigates existing security

DOI:http://doi.org/10.24086/cocos2024/paper.1491

challenges but also remains adaptable to evolving threats in the dynamic landscape of IoT and blockchain technologies. Therefore, all the studies are summarized in Table 1.

Table 1: Summarization of Literature reviews

Article	Key Findings/ Argument	Characteristics	Strength	Significance
[8]	In 5G and IoT systems, Blockchain's decentralized features provide a practical solution for improving security in device-to-device communication.	The EECDG approach utilizes the Grid Organizing Edge (EGE) algorithm to cluster IoT networks. The elected cluster head reduces energy for data transmission by minimizing the distance to member nodes. The winning sensor is chosen based on the best Euclidean distance.	EECDG addresses the critical issue of energy consumption in IoT networks, providing scalability and energy savings. The dynamic cluster head rotation approach extends network longevity and ensures balanced energy consumption.	Simulation results demonstrate EECDG's effectiveness; however, real-world validation is essential to assess its performance in practical IoT scenarios.
[7]	The article introduces SOA-FPC, a protocol using Self-Organizing Maps (SOM) and graph theory for cluster-based routing in dynamic IoT networks. It shows how machine learning-based clustering improves network lifetime, saves energy, and manages topology in IoT setups.	SOA is used for balanced clustering of sensor nodes, considering their dispersion. SOA-FPC integrates graph theory and artificial neural networks, specifically Self-Organizing Maps, for dynamic IoT network cluster-based routing.	The article doesn't detail the limitations of the SOA-FPC protocol, nor does it address the computational challenges of combining SOA and graph theory.	SOA-FPC boosts IoT networks by merging graph theory with neural networks, enhancing network lifetime and energy efficiency.
[9]	The study discusses issues related to next-generation networks and public safety communications in disaster management. The proposed method suggests using a combination of a hybrid adaptive neuro-fuzzy inference network-based genetic algorithm and an efficient routing Ingrid Optimization Algorithm.	The suggested disaster management plan uses a combination of Adaptive Neuro-Fuzzy Inference Network (ANFIS) and Genetic Algorithm (GA) for selecting cluster heads.	The paper thoroughly evaluates the suggested approach by comparing it to existing methods (Fuzzy and Epidemic) using various performance measures.	Future research in the field could be improved by a combination of different approaches, potentially leading to the creation of more efficient and flexible disaster management strategies.
[10]	The combination of IoT and blockchain technology can improve security in device-to-device communication. A multi-layer security protocol model using Evolutionary Computation techniques has been suggested to address deployment challenges.	The proposed security model for IoT networks in the 5G cellular system utilizes Blockchain technology and a decentralized architecture with K-unknown clusters generated through Evolutionary Computation methods. This approach provides a robust and multi-layered security solution by ensuring local authentication within clusters.	However, the use of decentralized systems and the complexity of Evolutionary Computation algorithms may lead to limitations in terms of processing requirements and memory usage. This could potentially impact the real-time performance of IoT devices with limited resources.	The suggested architecture is crucial for enhancing IoT network security in 5G networks by combining Evolutionary Computation methods and Blockchain technology. Implementation could lead to better data integrity, authentication, and communication reliability. However, deployment needs to take into account real-time constraints and available processing resources.
[24]	The study suggests that using blockchain technology in 5G-enabled IoT networks can effectively reduce security risks associated with smart devices. The proposed security architecture utilizes evolutionary computation and clustering to enhance security and simplify implementation.	The study uses a complex blockchain security approach for the IoT networks in the 5G era, utilizing decentralized technology. It includes clustering and evolutionary computation to enhance security and simplify implementation. Local authentication is managed by super nodes in private blockchains, while global communication is protected by a lightweight blockchain.	The proposed multi-level blockchain security model strengthens 5G-enabled IoT networks by incorporating decentralized technology, evolutionary computation, and clustering. This enhances security and trust through the use of both local and global blockchain systems.	A proposed multi-layer blockchain security approach is crucial for safeguarding 5G-connected IoT networks. Base security rules, offering enhanced trust and simplified deployment. This strategy seems to improve data integrity and authentication.
[11]	This article gives a detailed overview of current architectures and its applications in industrial and fifth-generation IoT scenarios. It also discusses the IIConIoT paradigm and highlights its potential to transform modern industry.	The paper explores combining blockchain technology with the Internet of Things (IoT) to tackle decentralization and security concerns, known as Blockchain of Things (BIoT). It provides a detailed examination of the BIoT architecture and its applications in industrial and fifth-generation IoT settings.	- The Blockchain of Things (BIoT) which combines blockchain technology and the IoT, offers a potent solution to problems with decentralization, interoperability, privacy, and security. This could lead to a paradigm shift in the use of data to inform decisions in smart industries.	The combination of blockchain technology and the Internet of Things (IoT), like Blockchain of Things (BIoT), has the potential to greatly impact industries by creating intelligent, data-focused ecosystems. This can lead to improved security, privacy, and compatibility in IoT applications. However, it is important to carefully consider the scalability and implementation challenges in order to fully harness the benefits of BIoT and drive innovation in different industrial sectors.
[12]	Blockchain technology is characterized by its transparency, immutability, traceability, and immutability. It has rapidly evolved, particularly in the realms of cryptocurrency and larger industries like manufacturing.	The approach includes introducing a new way of training, putting certain parts and functions into place, running tests in a controlled setting, and assessing how well the suggested cloud-edge collaborative fraud system works and its benefits.	The proposed cloud-edge collaborative fraud paradigm aims to improve scalability by releasing services to private cloud and on-premises edge settings, enhancing the dependability of blockchain systems in scenarios involving cross-timezone and edge scenarios.	This introduces a new cloud-edge collaborative approach that overcomes the limitations of existing fraud systems. It provides solutions to problems like vendor lock-in and scalability issues commonly found in traditional cloud-centric fraud systems.
[13]	One key advantage of blockchain technology is its capability to create an immutable and secure record of transactions, enhancing trust and reliability in business transactions.	The approach involves using a UML-based semi-model to guide users in developing smart contracts, prioritizing quality assurance and being adaptable to different programming languages. The goal is to improve compatibility and convenience while preparing for future updates to user-changing needs.	The advantages of implementing software quality assurance and using a UML-based meta-model as a starting point, but there are also challenges like potential complexity, a need for learning, and reliance on UML's relevance.	The importance of the suggested UML-based meta-model is that it could enhance communication, software quality assurance, interoperability, and adaptability in smart contract development. This could lead to the creation of trustworthy, low-error dependencies on specific vendors, and require education and training for widespread use.
[14]	Blockchain is considered a disruptive technology that has the potential to bring about significant changes in multiple industries. This recognition highlights the wide-ranging effects and transformative possibilities of blockchain in various scenarios.	This article discusses the potential impact of blockchain technology, the importance of evaluating different platforms, methods for assessing blockchain technology, and how to select the best techniques. The methodology includes a thorough survey and analysis of criteria to help make informed decisions and improve blockchain performance.	The paper needs to be thorough examination, organization, and identification of key factors, but it may be lacking in specific details or research methods, the nature of its analytical models, subjective evaluation, identification, the necessity for frequent updates, and practical examples of implementation.	Improving the efficiency and speed of blockchain technology. The paper offers a practical guide to improve the performance of blockchain by focusing on key evaluation criteria. This can potentially enhance the efficiency and effectiveness of blockchain implementations.
[15]	Blockchain technology is characterized by its transparency, immutability, traceability, and immutability. It has rapidly evolved, particularly in the realms of cryptocurrency and larger industries like manufacturing.	This approach includes introducing a new way of training, putting certain parts and functions into place, running tests in a controlled setting, and assessing how well the suggested cloud-edge collaborative fraud system works and its benefits.	The proposed cloud-edge collaborative fraud paradigm aims to improve scalability by releasing services to private cloud and on-premises edge settings, enhancing the dependability of blockchain systems in scenarios involving cross-timezone and edge environments.	This introduces a new cloud-edge collaborative approach that overcomes the limitations of existing fraud systems. It provides solutions to problems like vendor lock-in and scalability issues commonly found in traditional cloud-centric fraud systems.
[16]	This article highlights the economic security and privacy risks that can impact the IoT ecosystem enabled by 5G. It emphasizes the need to protect the infrastructure of the IoT environment by implementing various security measures such as key management.	This paper provides a detailed examination of previously and current security protocols in IoT environments powered by 5G. It focuses on system models, security specifications, potential threats, and various security procedures.	The article gives a comprehensive summary of the current state of security protocols in 5G-enabled IoT situations by bringing together and combining various research.	The literature review section of the study provides scholars and practitioners with an understanding of security issues and potential research directions for 5G-enabled IoT communications.

III. SELECTIVE IDEA OF MULTILAYER BLOCKCHAIN-BASED SECURITY

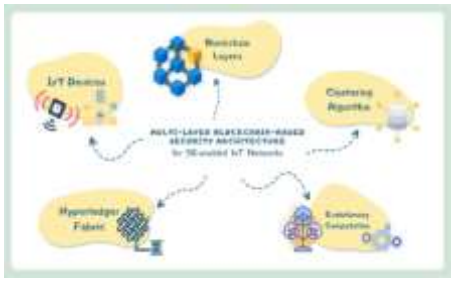

Figure 4: Multilayer Blockhain-Based Security

Figure 4 presents a comprehensive and creative security architecture that tackles the particular difficulties faced by IoT networks enabled by 5G. It highlights how crucial blockchain technology, evolutionary computation, clustering algorithms, and the Hyperledger Fabric platform are to bolstering security, privacy, and effectiveness in the rapidly changing IoT ecosystem. The components that are connected represent a unified strategy for dependable and safe communication throughout the IoT.

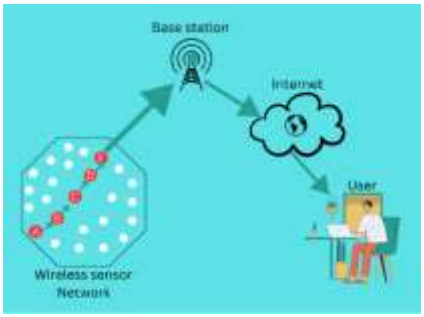

Figure 5: Wireless Sensor Networks (WSNs)

Figure 5 shows the function of Wireless Sensor Networks (WSNs) in relation to the IoT. WSNs are made up of networked sensors that gather environmental data and are essential to the IoT' ability to communicate and share data. Important WSN components, including sensor types, sensor nodes, and power supply issues. Aspects of wireless communication which also includes data transmission and reception as well as communication protocols.The section on network architecture emphasizes the significance of selecting between hierarchical and flat topologies, as well as centralized and distributed networks, while taking fault tolerance and scalability into account. This also highlights how important energy efficiency is to WSN design, since sensors are often placed in isolated areas with little access to electricity.It is also examined other uses of WSNs in IoT, including industrial IoT, smart homes, environmental monitoring, and healthcare. Wireless sensor networks (WSNs) in smart homes improve security by spotting potential threats and optimize energy use by using appliances.

DOI:http://doi.org/10.24086/cocos2024/paper.1491

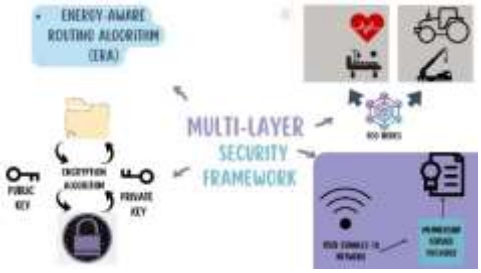

Figure 6: Multilayer Security Framework

Figure 6 explained about the framework aims to optimize energy consumption, reduce communication latency, and improve network coverage in IoT systems. The proposed framework utilizes a novel, lightweight, private multi-layer model tailored to meet the requirements of IoT devices. It leverages blockchain technology to provide secure communication and authentication for IoT devices. The architecture includes three layers: Layer-1 for IoT devices and nodes, Layer-2 for cluster heads and controlling devices, and Layer-3 for base stations in cellular networks. Key components of the framework include a clustering algorithm based on Genetic Algorithm (GA) and Simulated Annealing (SA), and the deployment of Hyperledger Fabric (HLF) blockchain technology. The proposed framework addresses challenges associated with blockchain implementation in IoT systems, such as device authentication, low scalability, transaction delays, and device heterogeneity. It aims to enhance network scalability, reduce complexity, and improve security for IoT devices. In summary, the document presents a comprehensive exploration of the multi-layer security framework for IoT networks, emphasizing the integration of blockchain technology, clustering algorithms, and smart contracts to address security, scalability, and performance challenges in IoT systems.

IV. STRATEGY OF INTEGRATION OF BLOCKCHAIN AND IOT IN SMART DEVICES

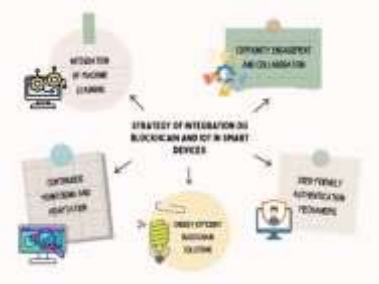

Figure 7: Strategy of integration of blockchain and Iot in smart devices

In figure 7, as the use of smart devices in the IoT increases, ensuring strong security is crucial. The proposed Multi-Layer Blockchain-Based Security Architecture for IoT networks suggests potential improvements to make the system more adaptable and aligned with the evolving needs of the IoT environment. Continuous monitoring and adaptation are necessary to track the changing dynamics of the IoT landscape and adjust the security architecture in real-time to emerging threats. This will help maintain the effectiveness of the security framework over time. The integration of machine learning can improve anomaly detection and predictive security analytics by analyzing device behavior patterns. This will help the system identify and respond to potential security issues more efficiently. Additionally, developing energy-efficient blockchain solutions is important for addressing the resource limitations of IoT devices and reducing computational overhead and energy consumption. In order to improve user authentication, it is important to find a balance between user-friendliness and strong security. This can be achieved by exploring biometric authentication or other simple methods that enhance user experience without compromising overall security. Additionally, fostering collaboration with the IoT community, researchers, and industry experts is crucial. By creating a collaborative environment, we can share findings, best practices, and innovations in IoT security, which will benefit the entire community.

V. CONCLUSION

In conclusion, the widespread adoption of smart device integration into IoT networks has resulted in notable security and privacy concerns that require creative solutions. To solve these issues, this study suggests a multi-layer blockchain-based security architecture for IoT networks that are 5G enabled. To improve security, privacy, scalability, and performance, the suggested design makes use of complex clustering techniques, decentralized and distributed blockchain technology, and a hybrid evolutionary computation algorithm. The introduction of K-unknown clusters using sophisticated clustering techniques, the creation of local private blockchains for safe intra-cluster communication, and the use of a global blockchain strategy for inter-cluster communication are among the main contributions of this work. The robustness of the suggested design is further confirmed by the implementation of the open-source Hyperledger Fabric Blockchain technology.

The results of the simulations demonstrate the efficiency of the clustering algorithm and the lightweight blockchain model's superiority over conventional global blockchain techniques in terms of balancing network latency and throughput. The suggested design addresses the shortcomings of the present blockchain implementations by providing a thorough and efficient security solution suited to the needs of IoT networks. For continued innovation and adaptation going forward, it is advised to include machine learning, energy-efficient blockchain solutions, user-friendly authentication methods, and community involvement with constant monitoring. By ensuring that the security architecture is durable and flexible enough to change with the IoT, these proposals hope to promote cooperation and group advancement among IoT security experts. Essentially, the Multi-Layer Blockchain-Based

DOI:http://doi.org/10.24086/cocos2024/paper.1491

Security Architecture that is being presented advances IoT security and establishes the groundwork for an IoT ecosystem that is more efficient, safe, and collaborative.

ACKNOWLEDGMENT

Special thanks are extended to the Centre of Excellence for Cybersecurity (CoExCys) at IIUM and the Silverseeds Lab Network for their invaluable support throughout this endeavor.

REFERENCES

[1] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, "IoT: Evolution, Concerns and Security Challenges," Sensors, vol. 21, no. 5, p. 1809, Mar. 2021, doi: 10.3390/s21051809.

[2] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in IoT with a focus on the impact of emerging technologies," IoT, vol. 19, p. 100564, Aug. 2022, doi: 10.1016/j.iot.2022.100564.

[3] T. Aljrees, A. Kumar, K. U. Singh, and T. Singh, "Enhancing IoT Security through a Green and Sustainable Federated Learning Platform: Leveraging Efficient Encryption and the Quondam Signature Algorithm," Sensors, vol. 23, no. 19, p. 8090, Sep. 2023, doi: 10.3390/s23198090.

[4] C. Butpheng, K.-H. Yeh, and H. Xiong, "Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review," Symmetry, vol. 12, no. 7, p. 1191, Jul. 2020, doi: 10.3390/sym12071191.

[5] M. A. H. Bin Haris, M. I. H. B. Yahya, and M. N. B. Ibrahim, "Security and Privacy Issues in IoT ," preprint, Jun. 2023. doi: 10.36227/techrxiv.23512389.v1.

[6] T. Yu, X. Wang, and Y. Zhu, "Blockchain Technology for the 5G-Enabled IoT Systems: Principle, Applications and Challenges," in 5G-Enabled IoT, 1st ed., Y. Wu, H. Huang, C.-X. Wang, and Y. Pan, Eds., CRC Press, 2019, pp. 301–321. doi: 10.1201/9780429199820-14.

[7] A. Abuashour, "An efficient Clustered IoT (CIoT) routing protocol and control overhead minimization in IoT network," Internet of Things, vol. 23, p. 100839, Oct. 2023, doi: 10.1016/j.iot.2023.100839.

[8] L. K. Murry, R. Kumar, and T. Tuithung, "Disaster management using D2D communication with ANFIS genetic algorithm-based CH selection and efficient routing by seagull optimisation," IJCSE, vol. 24, no. 4, p. 373, 2021, doi: 10.1504/IJCSE.2021.117017.

[9] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Multi-Layer Blockchain-Based Security Architecture for IoT," Sensors, vol. 21, no. 3, p. 772, Jan. 2021, doi: 10.3390/s21030772.

[10] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Multi-Layer Blockchain-Based Security Architecture for IoT," Sensors, vol. 21, no. 3, p. 772, Jan. 2021, doi: 10.3390/s21030772.

[11] F. Elghaish et al., "Blockchain and the 'IoT' for the construction industry: research trends and opportunities," Automation in Construction, vol. 132, p. 103942, Dec. 2021, doi: 10.1016/j.autcon.2021.103942.

[12] G. Tripathi, M. A. Ahad, and G. Casalino, "A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges," Decision Analytics Journal, vol. 9, p. 100344, Dec. 2023, doi: 10.1016/j.dajour.2023.100344.

[13] X. Zhang, "Blockchain Technology in Various Fields: Applications, Challenges, And Future," HSET, vol. 57, pp. 154–160, Jul. 2023, doi: 10.54097/hset.v57i.9994.

[14] A. Rejeb, K. Rejeb, S. Simske, and J. G. Keogh, "Exploring Blockchain Research in Supply Chain Management: A Latent Dirichlet Allocation-Driven Systematic Review," Information, vol. 14, no. 10, p. 557, Oct. 2023, doi: 10.3390/info14100557.

[15] J. Cook, S. U. Rehman, and M. A. Khan, "Security and Privacy for Low Power IoT Devices on 5G and Beyond Networks: Challenges and Future Directions," IEEE Access, vol. 11, pp. 39295–39317, 2023, doi: 10.1109/ACCESS.2023.3268064.