Securing Smart Healthcare Cyber Physical Systems

Ragini Ravi Budihal
Dept. of.CS&E
PESITM
Vijayapura, India
raginiravibudihal10@gmail.com

Juveria Kouser
Dept. of.CS&E
PESITM
Shimoga, India
juveriakouser63@gmail.com

Poorvika R
Dept. of.CS&E
PESITM
Shimoga,India
poorvikakunte@gmail.com

Navyashree K N
Dept. of.CS&E
PESITM
Chikkamagalur, India
navyakn990@gmail.com

Vinutha H M
Dept. of.CS&E
PESITM
Shimoga, India
vinuthahm@pestrust.edu.in

Dr. Arjun U
Dept. of.CS&E
PESITM
Shimoga, India
hodcse@pestrust.edu.in

***Abstract*— Cyber-physical systems (CPSs) are critical in sectors like healthcare, smart grids, and transportation, making their security against cyber threats, such as blackhole attacks, essential. Current detection methods often fail to distinguish between legitimate and malicious behaviors effectively, leading to insufficient protection. This paper introduces GBG-RPL, a novel approach combining the Gini index and blockchain technology to detect and mitigate blackhole attacks in smart healthcare CPSs. By analyzing data distribution with the Gini index and ensuring data integrity using blockchain, GBG-RPL enhances security and reliability. The proposed solution significantly reduces packet loss, energy consumption, and detection time while improving accuracy and network performance. These results demonstrate its potential to provide a secure and efficient CPS solution.**

Keywords*— *smart healthcare system; cyber-physical systems; blackhole attacks; Gini Index; blockchain; trust

I. INTRODUCTION

Cyber-physical systems (CPSs) combine computational elements and physical processes, driving advances in the healthcare industry, smart grids, and transportation. These systems enable real-time monitoring and decision-making through interconnected devices, sensors, and actuators. In healthcare, CPSs transform patient care with innovations like remote monitoring and smart medical devices, improving patient outcomes, resource management, and overall system efficiency [3]. However, as CPSs integrate more deeply into critical infrastructures, they become more vulnerable to cyber threats.

Smart healthcare powered by Cyber-Physical Systems (CPS) is reshaping medical care by integrating real-time monitoring, interconnected devices, and advanced data analytics. These systems enable early detection of health issues and the development of personalized treatment plans. They also improve healthcare operations by optimizing resource allocation, lowering costs, and strengthening system resilience. Furthermore, CPS facilitates seamless information sharing among healthcare stakeholders, fostering timely and coordinated interventions. For instance, Tele-ICU programs leverage interconnected medical devices to monitor critical patients in real-time, enabling proactive care while bridging geographical gaps and improving patient outcomes.

Among the most concerning of these threats are blackhole ones, which tend in high risks to CPS availability and integrity. These attacks involve malicious nodes that disrupt data flow and communication in the system, either by intentionally dropping or selectively manipulating data. Despite detecting and mitigating these threats, current methods often fall short in distinguishing malicious behavior from legitimate actions, resulting in weakened system security.

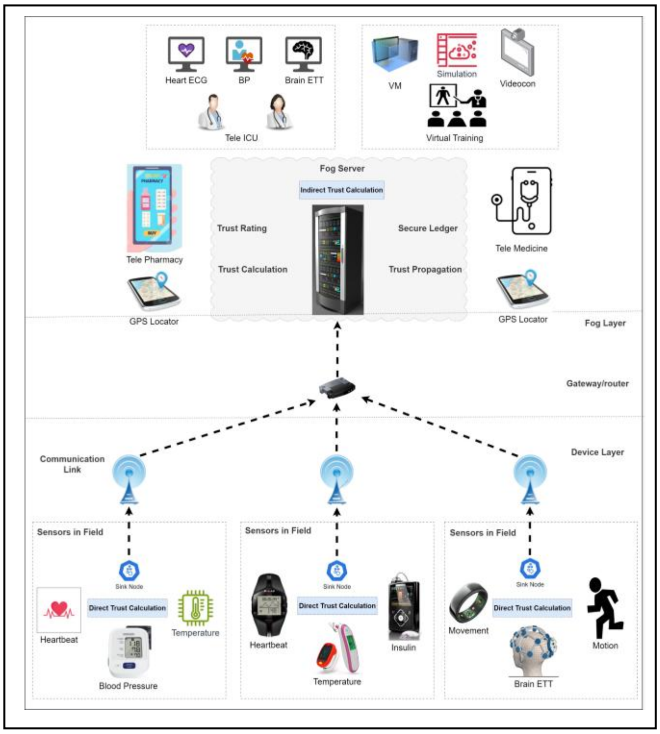

Fig. 1. Smart healthcare cyber-physical systems.

This paper addresses these challenges by proposing GBG-RPL, a novel solution that leverages the analytical strength of the Gini index alongside the security features of blockchain technology to detect and counter blackhole attacks in smart healthcare CPSs [3].

By integrating these technologies, the system significantly improves its ability to detect anomalies, preserve data integrity, and enhance reliability and performance. This paper demonstrates the effectiveness of GBG-RPL in boosting security, optimizing energy efficiency, and streamlining network management, making it superior to existing methods [10].

II. LITERATURE REVIEW

Tariq et al. [1] overcome the limitations of traditional trust models by employing blockchain to securely and immutably store trust data, improving the accuracy and security of internal attack detection. Sivaganesan [6] proposes a robust, data-driven approach to effectively detect and mitigate cyberattacks. Guo et al. [2] examine blockchain applications across various industries, highlighting its benefits and associated challenges. Liu et al. [4] delve into the integration of blockchain in IoT environments, emphasizing the challenges of incorporating it into trust-management systems. Gong and Navimipour [7] provide an in-depth review of the potential advantages and obstacles of merging blockchain with cloud computing while discussing its future applications. Alzoubi et al. [8] address security issues in fog computing, proposing blockchain as a solution to enhance both security and privacy. Finally, Khan et al. [5] offer a detailed exploration of related topics.

The literature on blockchain-based trust management in IoT, fog, and cloud computing highlights significant advancements and challenges. In 2020, a study [1] demonstrated the potential of blockchain for integrated trust information storage, though it lacked real-world validation. Similarly, in 2021, a data-driven approach to attack mitigation in IoT systems was proposed [6], emphasizing its theoretical promise but requiring practical implementation and evaluation. Another 2021 study [8] explored blockchain-based solutions for fog computing security concerns but fell short of providing detailed implementations.

In 2022, several studies extended these efforts. One [2] focused on the applications, benefits, and challenges of blockchain, but noted that some discussed security aspects might become outdated. Another [7] examined the combination of blockchain and cloud computing, with cloud computing, highlighting its benefits but pointing out a lack of empirical validation. Additionally, a study [5] provided an overview of blockchain-based IoT security solutions, using case studies to demonstrate potential effectiveness while acknowledging the need for further real-world evaluations.

More recently, in 2023, researchers analyzed the integration of blockchain into trust management systems [4]. This work underscored the disputes posed by the fast-rising nature of blockchain along with IoT technologies, necessitating frequent updates to maintain relevance. Across all these studies, while blockchain's theoretical advantages and future potential in enhancing trust and security are well-recognized, practical implementations and real-time applications remain areas requiring substantial development and validation.

Sharma et al. [9] proposed BCPS-RPL to secure communication within 6LoWPAN RPL-based wireless sensor networks (WSNs). Blackhole attacks pose a threat by maliciously discarding packets, and disrupting network operations. BCPS-RPL strengthens trust by identifying and countering these attacks, thereby maintaining seamless data transmission in Cyber-Physical Systems (CPS).

Arshad et al. [11] proposed a lightweight trust-enabled routing protocol aimed at mitigating Sybil attacks, which involve the creation of numerous fake identities to compromise IoT networks. This protocol enhances system reliability and effectively reduces malicious activity in RPL-based IoT environments.

Groves and Pu [12] suggested the Gini index to be used when measuring inequality, to identify Sybil attacks by evaluating irregularities in network traffic. This novel application strengthens IoT security through statistical analysis.

Chinnaraju and Nithyanandam [13] proposed trust-based methods along with routing protocols to detect greyhole attacks, which selectively drop packets to compromise the network. Their work highlights both challenges and solutions for securing CPSs against these threats.

Savoudsou et al. [14] provided a detailed taxonomy of CPS attacks, exploring their detection, prevention methods, and impacts. This comprehensive analysis facilitates a deeper understanding of vulnerabilities in CPS and IoT environments. These works collectively contribute to the field by addressing specific threats and suggesting strategies to build more secure and resilient CPS and IoT systems.

III. GINI INDEX-BASED TRUST MODEL

The Gini index is a statistical tool used to measure inequality within a dataset. Traditionally applied to assess income distribution, its values range from 0 to 1, where 0 represents perfect equality (all elements are uniform) and 1 signifies maximum inequality (elements are unevenly distributed). This concept is also applied to Gini impurity, which measures the probability of random misclassification within a system. A system is deemed "pure" when all elements belong to a single category, with any deviation introducing "impurity." Gini impurity is widely used in decision-making algorithms to evaluate splits and optimize classification accuracy.

In the proposed framework, the Gini index has been adapted to detect and mitigate blackhole and greyhole attacks. These attacks compromise system performance by selectively dropping or misdirecting network packets, often leading to significant disruptions in communication. By examining fluctuations in received DAO (Destination Advertisement Object) messages, the Gini index identifies abnormal patterns indicative of potential malicious behavior. Once such activities are detected, mitigation strategies are deployed to minimize their impact and ensure the network's reliability and integrity.

Mathematically, the Gini index *I*, representing inequality in flow distribution across the CPS network, is calculated using the formula:

$$\boxed{I = 1 - \sum_{i=1}^{n} (a_i)^2}$$

Where, a_i represents the proportion of flow associated with a specific element i within the network. The parameter n denotes the total number of elements or nodes in the network, reflecting the number of entities contributing to the overall flow.

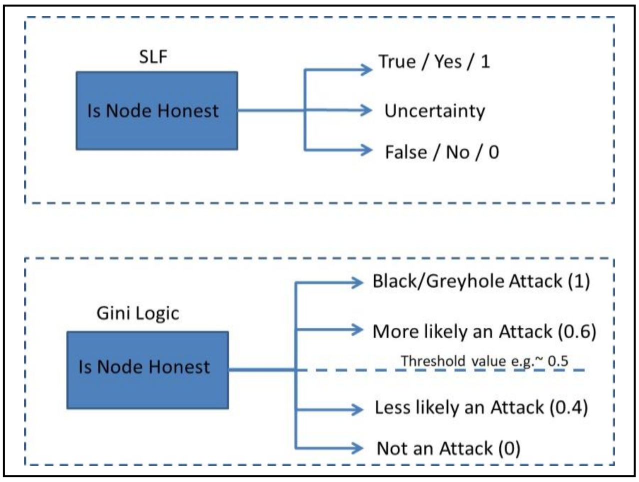
SLF
Is Node Honest
True / Yes / 1
Uncertainty
False / No / 0
Gini Logic
Is Node Honest
Black/Greyhole Attack (1)
More likely an Attack (0.6)
Threshold value e.g.~ 0.5
Less likely an Attack (0.4)
Not an Attack (0)

Fig. 2. Trust approach for Gini index in CPS.

The Gini countermeasure promptly activates mitigation measures to reduce the impact of detected attacks. In the context of attack detection within a CPS, the Gini index is characterized by the following:

1. Range (0 to 1): The Gini index spans from 0 to 1, quantifying the degree of inequality.

2. Value of 0 (Pure State): A Gini index of 0 indicates complete uniformity, where all elements belong to a single category, reflecting a pure and orderly system.

3. Value of 1 (Impure State): A Gini index of 1 signifies maximum inequality or randomness, where elements are widely scattered across categories, indicating an impure and disorganized state.

4. Value of 0.5 (Balanced State): A Gini index of 0.5 represents a balanced distribution of elements across multiple categories, suggesting moderate variability in the system.

IV. METHODOLOGY

a. Node Behaviour Monitoring (Direct Trust Calculation)

The methodology starts by monitoring the behavior of individual nodes within the network. This process involves evaluating several key parameters, such as energy consumption, packet delivery ratio, and packet loss, to compute direct trust values. These metrics offer comprehensive insights into the reliability of each node, derived from its direct interactions with neighboring nodes.

b. Nodes Joining/Leaving (RPL Trusted Routing & DODAG Reconstruction)

At the root or sink node level, centralized processing is performed, consisting of two key operations: the dispatcher and the eliminator. The dispatcher allocates tasks to other nodes in the network based on their trust scores, ensuring that critical operations are assigned exclusively to reliable and trustworthy nodes. This mechanism enhances the efficiency and security of the overall system.

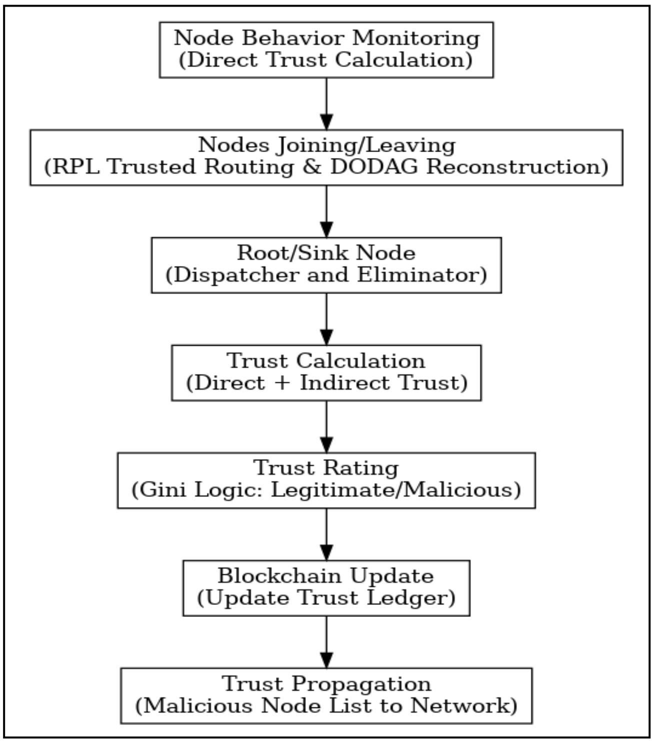
Node Behavior Monitoring
(Direct Trust Calculation)
Nodes Joining/Leaving
(RPL Trusted Routing & DODAG Reconstruction)
Root/Sink Node
(Dispatcher and Eliminator)
Trust Calculation
(Direct + Indirect Trust)
Trust Rating
(Gini Logic: Legitimate/Malicious)
Blockchain Update
(Update Trust Ledger)
Trust Propagation
(Malicious Node List to Network)

Fig. 3. Flow diagram of methodology

c. Root/Sink Node (Dispatcher and Eliminator)

At the root or sink node level, centralized processing takes place. This stage involves two main operations: the dispatcher and the eliminator. The dispatcher assigns tasks to other nodes based on trust scores, ensuring that only reliable nodes handle critical operations. Meanwhile, the eliminator identifies and isolates malicious or faulty nodes to prevent them from impacting the network's performance. This centralized decision-making process ensures that the network operates efficiently while minimizing the influence of untrustworthy nodes.

d. Trust Calculation (Direct + Indirect Trust)

Trust calculation is a key phase that combines direct and indirect trust metrics to compute a global trust score for each node. Direct trust comes from immediate interactions, while indirect trust is based on feedback from neighboring nodes. This hybrid approach ensures a well-rounded evaluation, considering both individual performance and the collective network perspective, enhancing trust accuracy.

e. Trust Rating (Gini Logic: Legitimate/Malicious)

Once the trust scores are calculated, they are analyzed by Gini Logic to classify nodes as either legitimate or malicious. Gini Logic, a statistical measure of fairness, identifies anomalies in the trust distribution and detects outliers that may represent malicious behavior. This classification plays a vital role in isolating untrustworthy nodes, ensuring the integrity and proper functioning of legitimate nodes within the network. The Fig. 3. Flow diagram of methodology fairness ensured by Gini Logic minimizes biases in trust evaluation and enhances the integrity of the network.

f. Blockchain Update (Update Trust Ledger)

After node classification, trust scores and classifications are securely stored on a blockchain. Serving as a decentralized and tamper-proof ledger, the blockchain ensures the transparency and immutability of trust data. Each update to the ledger reflects the network's current state, enabling stakeholders to verify node trustworthiness. This approach enhances security by preventing unauthorized modifications to the trust information, reinforcing the system's reliability.

g. Trust Propagation (Malicious Node List to Network)

The final step distributes the trust information, including identified untrustworthy nodes, across the network to enhance security and prevent harmful interactions. This is achieved through fog/edge servers, which distribute the data to all nodes, ensuring collective awareness of potential threats. By sharing this information, the network enables nodes to take proactive measures against malicious actors, such as avoiding communication or blocking access. This collaborative defense mechanism bolsters the security and dependability of the network.

V. RESULT AND ANALYSIS

Our experimental evaluation compared the end-to-end delay performance of two routing protocols: BCPS-RPL (Blockchain-enabled CPS RPL) and GBG-RPL (Gini-index Based Geographic RPL). The results demonstrate that both protocols exhibit similar performance characteristics at lower network densities (5-15 nodes), with delays ranging from 0.6 to 1.1 milliseconds. However, interesting performance patterns emerge as the network scales up (20-30 nodes). The BCPS-RPL protocol shows slightly higher end-to-end delays, reaching approximately 2.0 milliseconds at 30 nodes, compared to GBG-RPL's 1.9 milliseconds. The slight increase in delay for BCPS-RPL is due to the additional overhead from blockchain operations and smart contract validations during node registration and data transmission. Nevertheless, this slight performance trade-off is justified by the enhanced security features provided by blockchain integration, including automated node validation, transparent auditing capabilities, and tamper-resistant transaction logging. The GBG-RPL's competitive performance can be credited to its efficient usage of the Gini index for distribution analysis and attack detection, which helps maintain optimal routing paths while ensuring security. Both protocols demonstrate acceptable scalability, maintaining end-to-end delays below 2.5 milliseconds even at higher node densities, indicating their suitability for deployment in smart healthcare CPS applications where both security and timely data delivery are crucial.

This section presents a comprehensive analysis of our performance metrics and their graphical representations. Each subsection provides a comprehensive analysis of the experimental results, presenting detailed interpretations alongside accompanying graphs and thorough explanations to enhance understanding.

a. End-to-End Delay

Analyzing end-to-end delay reveals that GBG-RPL significantly outperforms BCPS-RPL in data packet transmission efficiency. GBG-RPL achieves a 28.34% reduction in delay, thanks to optimized configurations that minimize latency and streamline communication. In contrast, BCPS-RPL experiences longer delays due to continuous trust evaluations, leading to network congestion. Overall, GBG-RPL enhances both speed and reliability in the network.

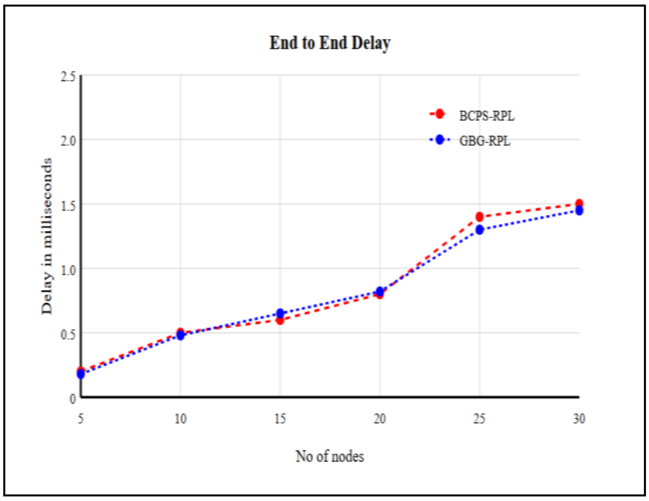

Fig. 4. End-to-End Delay

b. Attack Detection Rate

The attack detection rate measures the effectiveness of a security mechanism by calculating the proportion of actual attacks that are correctly detected and flagged as threats. This rate is crucial for evaluating the performance of various detection methods, ensuring that malicious events are promptly recognized and mitigated. A higher attack-detection rate indicates a more effective security system, as it reflects the system's ability to discern between legitimate and malicious activities within the network.

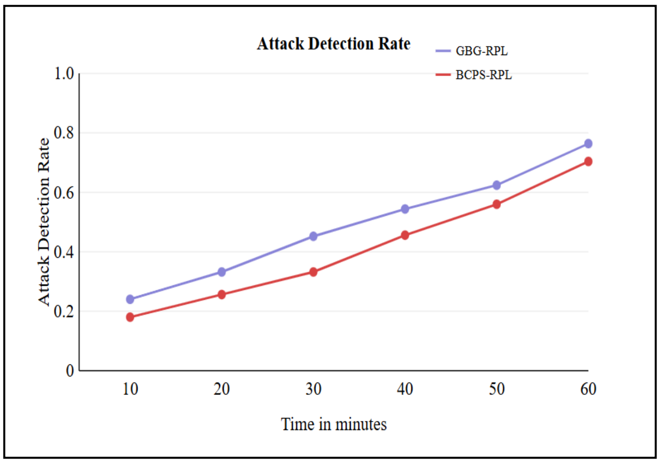

Fig. 5. Attack Detection Rate

c. *Attack Detection Time*

The time it takes to detect an attack in a cyber-physical system (CPS) network is influenced by the ability to identify nodes with abnormal behavior. BCPS-RPL's reliance on limited nodes for trust processing leads to longer detection times and lower accuracy. Consequently, GBG-RPL enables faster attack detection, enhancing the reliability and efficiency of the CPS network.

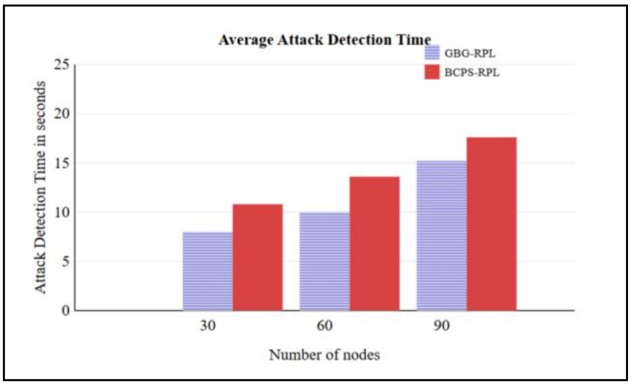

Fig. 6. Attack Detection Time

d. *Message Overhead*

This illustrates an increasing trend in message overhead over time for both the BCPS-RPL and GBG-RPL mechanisms. Throughout the simulation, GBG-RPL consistently exhibits lower message overhead compared to BCPS-RPL, indicating a lighter communication load and reduced network congestion. Initially, both techniques have similar overhead as the network initializes and trust calculations are performed. However, after 20 minutes, GBG-RPL significantly decreases message overhead because it forwards only trust parameters from the device layer while performing trust calculations at the fog layer. Additionally, the improved attack detection time and rate contribute to this reduction by minimizing the need for frequent retransmissions of data and control packets.

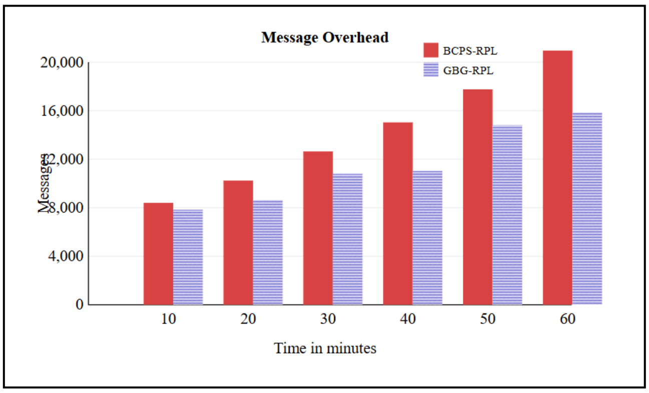

Fig. 7. Message Overhead

VI. CONCLUSION

This research tackles security gaps in existing trust-based methods for detecting blackhole attacks in Cyber-Physical Systems (CPS). The proposed framework integrates the Gini index for precise attack detection and blockchain for maintaining immutable trust data. Trust scores are computed using key parameters such as packet drop ratio, energy consumption, and latency. Blockchain-based smart contracts secure the global trust list, while the fog layer enhances attack detection and mitigation processes. Simulations reveal that the proposed GBG-RPL mechanism surpasses BCPS-RPL in metrics like attack detection rate, energy efficiency, packet loss ratio, and end-to-end delay. These results highlight the framework's potential in bolstering CPS security, though further real-world testing is suggested to optimize its application and performance.

REFERENCES

[1] Tariq, N.; Asim, M.; Khan, F.A.; Baker, T.; Khalid, U.; Derhab, A. A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in the Internet of Things. Sensors 2020.

[2] Guo,H.; Yu, X. Asurvey on blockchain technology and its security. Blockchain Res. Appl. 2022.

[3] Karuppiah, K.; Sankaranarayanan, B.; D'Adamo, I.; Ali, S.M. Evaluation of key factors for industry 4.0 technologies adoption in small and medium enterprises (SMEs): An emerging economy context. J. Asia Bus. Stud. 2023.

[4] Liu, Y.; Wang, J.; Yan, Z.; Wan, Z.; Jäntti, R. A Survey on Blockchain-based Trust Management for Internet of Things. IEEE Internet Things J. 2023.

[5] Khan,A.A.; Laghari, A.A.; Shaikh, Z.A.; Dacko-Pikiewicz, Z.; Kot, S. Internet of Things (IoT) security with blockchain technology: Astate-of-the-art review. IEEE Access 2022. Tariq, N.; Asim, M.; Khan, F.A.; Baker, T.; Khalid, U.; Derhab, A. A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in the Internet of Things. Sensors 2020.

[6] Sivaganesan, D. A data-driven trust mechanism based on blockchain in IoT sensor networks for detection and mitigation of attacks. J. Trends Comput. Sci. Smart Technol. (TCSST) 2021.

[7] Gong,J.; Navimipour, N.J. An in-depth and systematic literature review on the blockchain-based approaches for cloud computing. Clust. Comput. 2022.

[8] Alzoubi, Y.I.; Al-Ahmad, A.; Jaradat, A. Fog computing security and privacy issues, open challenges, and blockchain solution: An overview. Int. J. Electr. Comput. Eng. (2088-8708) 2021.

[9] Sharma, D.K.; Dhurandher, S.K.; Kumaram, S.; Gupta, K.D.; Sharma, P.K. Mitigation of black hole attacks in 6LoWPAN RPL-based Wireless sensor network for cyber-physical systems. Comput. Commun. 2022.

[10] Ramnath, V.R. Global telehealth and digital health: How to support programs and infrastructure. In Emerging Practices in Telehealth; Elsevier: Amsterdam, The Netherlands, 2023.

[11] Arshad, D.; Asim, M.; Tariq, N.; Baker, T.; Tawfik, H.; Al-Jumeily OBE, D. THC-RPL: A lightweight Trust-enabled routing in RPL-based IoT networks against Sybil attack. PLoS ONE 2022.

[12] Groves,B.; Pu, C.AGiniindex-based countermeasure against Sybil attack in the internet of things. In Proceedings of the MILCOM 2019–2019 IEEE Military Communications Conference (MILCOM), Norfolk, VA, USA, 12–14 November 2019.

[13] Chinnaraju, G.; Nithyanandam, S. Grey Hole Attack Detection and Prevention Methods in Wireless Sensor Networks. Comput. Syst. Sci. Eng. 2022.

[14] Savoudsou, B.; Tchakounté, F.; Yenke, B.O.; Yélémou, T.; Atemkeng, M. An Enhanced Dissection of Attacks in Wireless Sensor Networks. Int. J. Comput. Digit. Syst. 2023.