

Block chain Based Authentication Scheme for Secure Internet of Things Networks

Nitesh Kumar Saxena^{1*} , Mr. Pulkit Srivastava² , Viksit Tripathi³ 
^{1,2,3}Invertis University, Bareilly-243123, India

*Corresponding Author Email: niteshsaxena2005@gmail.com



This is an open-access article distributed under the terms of the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

The Iota has revolution modern applications by allowing smart devices in healthcare, smart home, transportation, agriculture, and industry automation to be connected collectively. However, the quantity of connected things has grown rapidly, which has posed severe security and privacy issues, notably given the limited computational resources, storage, and energy. The traditional centralized authentication processes suffer from various security risks, including single points of failure, unauthorized access, and data tampering. To address these challenges, we present in this paper a lightweight block chain-based authentication scheme for secure Iota environments. The architecture exploits the block chain technology to enable decentralized device registration and authentication without a trusted third party. It combines gateway and miner nodes to verify authentication requests and hold device data on the block chain with security. Various lightweight cryptographic primitives, such as Elliptic Curve Cryptography (ECC) operation, SHA-256 hashing, digital signatures, timestamps, and nonce's, are used to maintain confidentiality, integrity and authenticity, prevent against replay attacks and reduce the computation cost. The proposed authentication scheme is analyzed using the AVISPA security verification tool, which shows that it is secure against most popular attacks. Simulation results show that the proposed framework outperforms for better security, scalability, privacy and adaptability and it is appropriate for resource constrained Iota devices. The proposed approach enables an effective and trustworthy authentication solution for secure future Iota networks.

Keywords: Block chain, Internet of Things, Lightweight Block chain, Security, Privacy, Authentication scheme

1.0 Introduction

A block chain-based authentication protocol is proposed, which makes use of the idea of block chain to authenticate the Iota devices in a secure manner. The network permits only trusted devices. The system halts hacking and spoliation of data. It improves security, trust, and privacy over Iota messaging. It also provides a decentralized and transparent authentication mechanism. Applications of 803.15.4 to Iota in the recent years, many researchers have suggested Iota user authentication schemes that are based on block chain characteristics such as decentralization, security, and transparency to solve issues like data confidentiality, scalability, and centralization. These applications replace traditional centralized servers with a distributed network to guarantee a safe, tamper-evident, authentication process. Users can be authenticated with digital signatures and access control policies can be enforced using smart contracts, also the use of public/private key pairs is essential in user registration. The algorithms of consensus that are used by block

chain allow for real time auditing and monitoring as well as the validation of the authorization requests. Yet, it is crucial to tackle issues like scalability, privacy challenges, resource limitations on Iota devices, and latency. These problems are addressed head-on by Iota applications such as smart homes, healthcare, industrial Iota, and supply chain management. Yet it is possible to provide strong solutions that are secure, scalable and suitable for decentralized authentication for block chain systems. [1]. Due to the proliferation of Iota nodes, it is now a pressing challenge to deal with the scalability, privacy, and security issues for the sustainable development of this technology. A three-layer architecture, which is the most primitive type of Iota architecture, is shown in Figure 1 [2]. They are the perception layer, the network layer and the application layer.

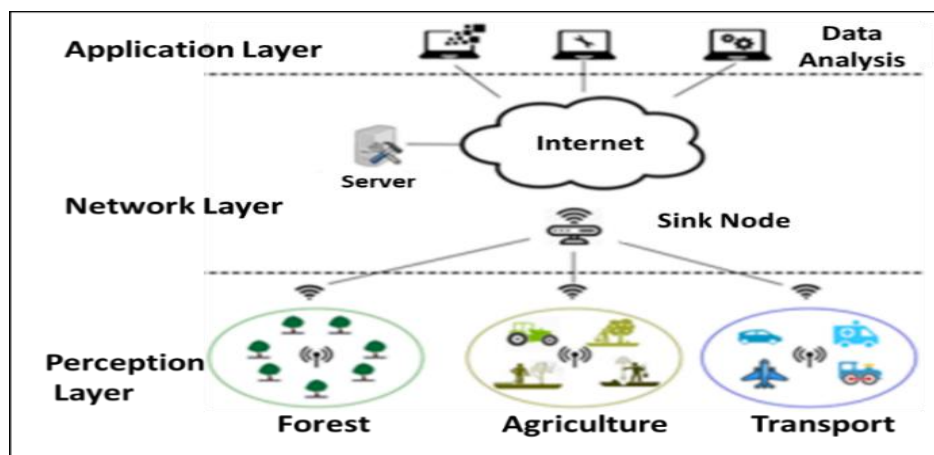


Figure 1: Three-layer Iota Architecture

Availability, scalability, flexibility, management, efficiency, security, and privacy are the matters of concern for Iota systems. Security is alive and well in the real world. The Iota should protect sensitive data transfers. Iota security can be enhanced with block chain. Many security techniques such as Block chain are not feasible for Iota due to Iota resource and energy limitations. The expanding size of the Iota ecosystem has generated concerns over privacy and security. Resource-limited and energy-harvesting Iota devices are the impediment of security and privacy. A few years ago, researchers have been leveraging block chain technology to surmount limitations in the Iota ecosystem. Due to its decentralized nature, block chain can potentially eliminate a number of the limitations of Iota and make the framework more efficient.

Block chain is Distributed Ledger Technology (DLT) [3], and it uses a P2P network to maintain and update a secure ledger database. Digital ledger technology records value and asset transactions. Unlike centralized data storage and administration, distributed ledgers simultaneously log data in multiple locations. With Block chain, distributed ledgers have Hash graphs and IOTA [4]. Transactions are batched into blocks, connected to each other with cryptographic hash functions as a “block chain”. Bit coin and Ethereum are crypto currency block chains. As a result of Thorium’s ability to run smart contracts, the definition of Block chain applications has been extended. Ethereum is unique as a consensus-based global virtual computer, which has its own programming language Solidity. There are many platforms that are suitable for creating Block chain-based apps, including Ethereum, as well as a few others. Technologies, such as Hyper ledger Fabric, Multichip, Quorum, Lick and HDAC (hierarchical deterministic application chains) [5]. The most active block chains were hyper ledger, Ethereum and Multichip. Figure 2 shows the basic block chain block structure [6]

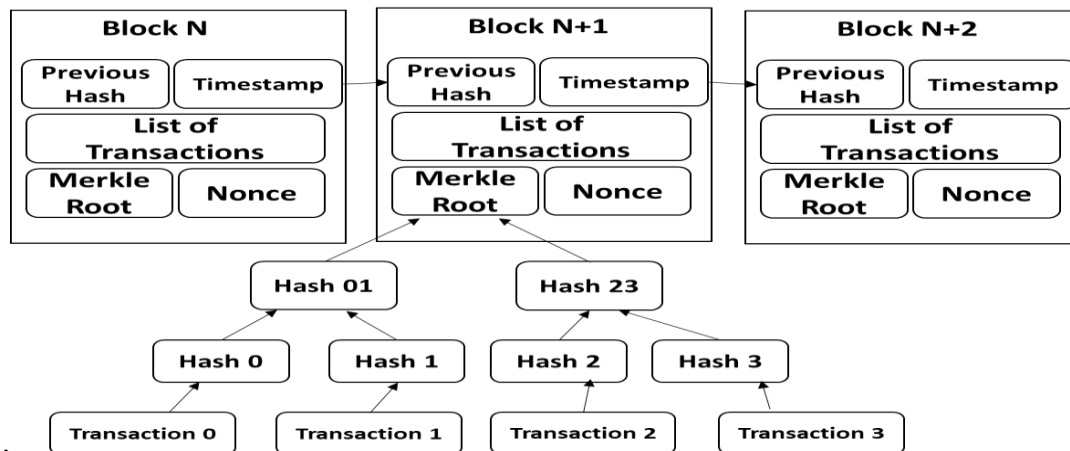


Figure 2: Structure of a Block chain and Merle Tree for Transaction Verification

The advantages of Block chain technology make it a perfect option for tackling the concerns that are associated with the Iota, especially those that pertain to security. Existing implementations of Block chain, on the other hand, are not compatible with the Iota, which presents the potential to further enhance the system that is now in place. The following research topics need to be concentrated on to address the difficulties that have arisen as a result of the confluence of block chain technology with the Iota: 1. The Iota and Block chain have come together to provide a new scope for study. It is not possible to directly integrate existing Block chain designs as an Iota network that is built on Block chain. A new secure Block chain design is needed to support Iota and other secure architectures. 2. Current Block chain implementations use ECC and SHA256 cryptography. These techniques are unsuitable for Block chain-based Iota deployments because Iota devices have limited resources and time. To integrate the Block chain-based idea in Iota designs or other related architectures and make the system secure, lightweight cryptographic techniques must be investigated [6].

The primary purpose of this study is to build a lightweight Iota architecture that is based on Block chain technology. This architecture will assist in improving the overall performance of a network that is limited in its resources. The difficulties associated with the merging of block chain technology with the Iota have opened up new avenues for study. The research aims of this study are as follows, and they are based on the research topics that have been presented:

1. To create Iota architecture that is based on Block chain technology.
2. To modify security protocols that are appropriate for architectures based on block chain technology and to conduct performance evaluations of the architecture that has been offered.

2.0 Related Works

Almadhoun et al. [7] presented an authentication system for users, in which block chain-enabled fog nodes make use of ethereal smart contracts to authenticate users to get access to Iota devices. In this context, fog nodes contribute to the reduction of heavy processing for activities like identification and communication with the block chain being carried out by Iota nodes.

Musher et al. [8] presented a technique that is based on block chain technology by enabling user authentication access to fog-enabled Iota devices. Additionally, Ethereum Smart Contracts were used in the implementation of this strategy.

Y. Liu et al. [9] first proposed a block chain-based cross-domain authentication management solution for Iota devices. The Merle tree stores sensitive device data, and only the Merle root is submitted to the smart contract. Second, a thorough security and performance study. They demonstrate that the system is genuine, active, and safe against many attacks. They achieved decentralization, privacy, scalability, rapid off-chain authentication, and cheap on-chain storage compared to previous systems. Third, they build the system on Ethereum with variant domains, concurrent authentication requests, and Merle tree leaf numbers.

R. Kumar et al. [10] used block chain-based AKA and explainable AI (XAI) to secure smart city consumer apps. Firstly, they used a block chain-based AKA mechanism, the involved organizations securely exchange data. However, they employed Shapley additive explanations (SHAP) to explain and analyze the most important choice factors. The framework's actual implementation shows its efficiency over current state-of-the-art methods.

P. Zhang et al. [11] proposed a block chain-based Iota-based collaborative processing system for maritime transportation flow scheduling and management. To lower block chain consensus communication costs, they proposed a new consensus method based on Verifiable Random Function (VRF) and reputation voting. A simulation showed that the suggested technique resists replay and camouflage attacks. Assuming unaltered communication costs, the optimized consensus technique increases security by 8% and transaction processing speed by 6%.

X. Jiao et al. [12] introduced Privacy-aware entity authentication and proposed a fog computing-based block chain-assisted authentication system for Iota applications. Considering entity capacity, they offer two privacy-preserving authentication algorithms based on elliptic curve cryptography (ECC) and physically inclinable functions (PUFs). Security analysis and performance assessment showed that the suggested protocols have competitive computation and communication costs while meeting security criteria.

Within the framework that was suggested by Ashen et al. [13], the Iota devices and end-users are authenticated using a server that is located locally. Additionally, the localized server helps in the execution of intensive computing tasks for end users, which in turn reduces the burden on the Iota devices. The information that is used for authentication is subsequently stored on the block chain and dispersed among the many nodes of the system [14].

3.0 Proposed Method

This study introduces a block chain-based authentication system for Internet of Things (Iota) architecture. The Block chain, as well as the registration of miner nodes. From the design, it can be inferred that the miner is a node with superior computational capacity. The mining node is tasked with authenticating the credentials of the user, gateway, and devices. Figure 3 illustrates the communication diagram employed within the organization.

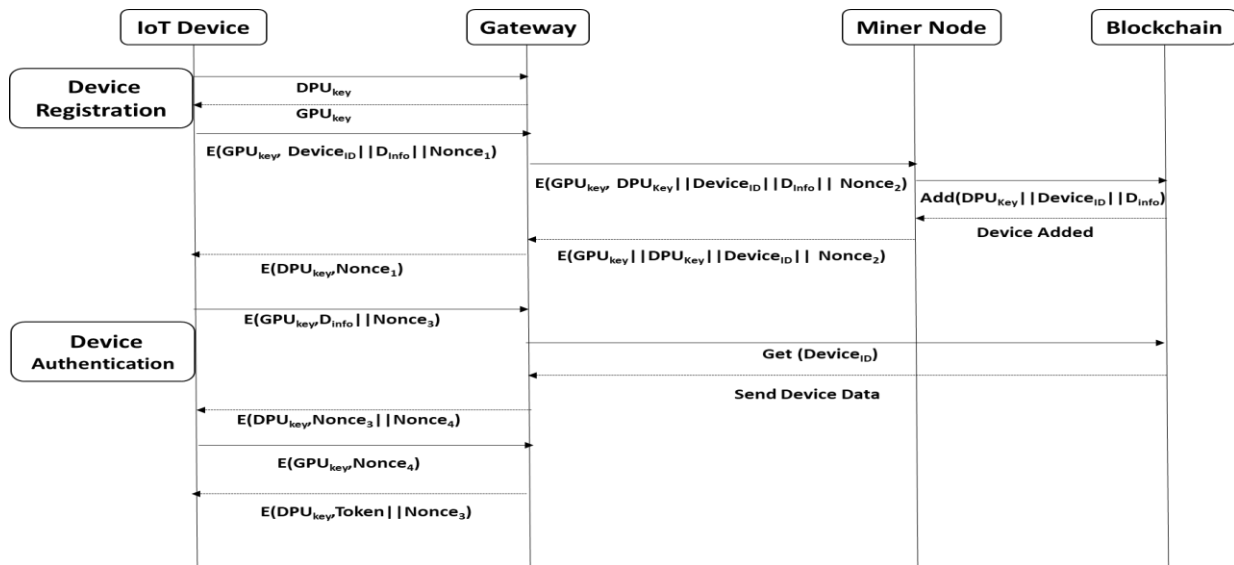


Figure 3: Block chain-based Authentication scheme for Iota Device

Block chain authentication can verify the identification of a user, device, or system within the block chain network. The integration of Internet of Things (Iota) with block chain technology has the potential to significantly transform various industries by enabling secure, transparent, and efficient data exchange. Iota devices enable businesses to collect and transmit data instantly, while block chain provides a decentralized and unchangeable system for storing and sharing data.

3.1 Device Registration:

Devices are the identifiers that are used to identify Iota devices. Following the completion of the device registration process, the user will be provided with a D_{opey} , which is the private key for configuring the device. An ECC public key, also known as a D_{uke} , is obtained from the private key that the user shares with the system.

The Iota device verifies its own identity by submitting a request to the gateway, which holds the device's public key, also known as the D_{uke} . Glu_{ey} is the gateway's public key, which it uses to respond to requests. After that, the device transmits the device ID, which is denoted by the acronym "Devised," in addition to the device information, which is denoted by "Dingo," and the nonce, which is denoted by "Nonce1." It is the gateway public key $E(Glu_{ey}, Devised || D_{ingo} || Nonce_1)$ that is responsible for encrypting this communication. It is with the help of the timestamp ($Time_{s1}$) that the intruder is prevented from keeping this request and retrieving it at a later time. It is expected that the message will be formatted as follows: $E(MPK, Devised || D_{ingo} || Nonce_1 || Time_{s1})$. With the help of the timestamp ($Time_{s1}$), the gateway determines whether or not this is a request that was made recently. The gateway performs an internal validation of the request and then sends a registration request to the miner node. This request includes the following information: $E(Glu_{ey}, D_{uke} || Devised || D_{ingo} || Nonce_2)$. To authenticate the communication, the nonce, ($Nonce_2$) is used as a challenge. This will assist in the prevention of the replay attack. The miner node is the recipient of the registration request that has been encrypted. After that, it determines whether or not the identification of the device is present on the Block chain.

If the user registers the device, the miner node will upload the device's public key and device information ($D_{uke} || Devised || D_{ingo}$) to the Block chain. The miner node is responsible for transmitting the device public key, the device ID, and the nonce to the gateway. The gateway public key $E(Glu_{ey} || D_{uke} || Devised || Nonce_2)$ is then used to encrypt the message to ensure its

integrity. The value of $Nonce_2$ is checked by the gateway, and if it is found to be legitimate, the gateway sends a response that includes the device ID and the gateway public key ($Devise_d$), as well as the Glu_{ey} to the device $E(Duke, Devise_d || Glu_{ey} || Nonce_1)$.

3.2 Device Authentication

An encrypted message with the message $E(Glu_{ey}, D_{ingo} || Nonce_3)$ is sent by the Iota device to the gateway to authenticate the gateway's request for the device information to be sent to the block chain server. To communicate with the gateway, the block chain sends the information about the specific device. This request would be authenticated by the gateway, which would determine whether or not it was received from the same device ID that was transferred in the first request. After the receipt of the authentication, the gateway will make the device authorized.

SHA-256 is the hash function that is employed as the consensus algorithm since the traditional Block chain scheme has been imposed as the security system that has been applied to the Iota architecture. At this point, the Masters, who are the mining nodes, also produce random public and private key pairs using the Digital Signature Algorithm (DSA), which contributes to the generation of one-of-a-kind signatures using the original data. The workers, also known as lightweight nodes, are provided with the information using the Base64 encoding standard, as well as the specifics of the Block chain and the digital signature properties. The workers can verify that the data is coming from a genuine source by using the public key of the masters that they have received. Any other key that is used will result in the data being rejected. To prevent the development of a private key via the use of brute force methods, the public-private key pair in this scenario is maintained dynamically in each block. In addition, the workers verify each block and its hash by mining the nonce value. This process is carried out by the workers. If any worker detects an issue in terms of tampering with the Block chain or forging signatures, the Block chain that is used by the majority of the network will be transferred to that specified node.

4.0 Performance Evaluation

The integration of Block chain technology can significantly influence the Iota ecosystem, particularly in terms of privacy and security aspects. Utilizing lightweight cryptography enables the resolution of numerous challenges presented by the Iota without excessively straining the capabilities of Iota components. This ensures compatibility with real-time applications. We proposed an adaptable authentication system that can be integrated into block chain architecture. The suggested design was used as a basis for conducting a performance study and protocol assessment, with the use of the AVISPA program (Automated Validation of Internet Security Protocols and Applications). The results demonstrate that the system is robust and safeguarded against any potential attacks.

Table 1 presents a concise comparison of the proposed system with established block chain-based Iota security approaches.

Table 1: Comparison of Security Parameters

References	Security Parameters				
	Authentication	Access Control	Adaptability	Integrity	Privacy
Labia et al. [15]	Yes	Yes	No	Yes	Yes
Mali et al. [16]	Yes	Yes	No	Yes	No
Kosice et al. [17]	Yes	Yes	No	Yes	No
Rather et al. [18]	Yes	Yes	No	Yes	No
Latin et al. [19]	Yes	Yes	No	Yes	Yes
Proposed Method	Yes	Yes	Yes	Yes	Yes

Integration of block chain technology into Iota environments provides many advantages that can aid in overcoming performance constraints and ensuring data integrity and trust, including decentralization, scalability, and security.

5.0 Conclusion

Additionally, the Iota environment is attracting attention, and research is being conducted actively. Authentication is something that has to be taken into consideration since the Iota ecosystem is intimately tied to personal information, it contains a huge number of devices, and all of the devices are connected to the Internet. Nevertheless, in the case of the present authentication protocols for the Iota, there is inadequate consideration for low-performance devices that employ central processing units (CPUs) that do not have built-in encryption or that are unable to conduct public key cryptography. As a result, in this work, we suggested a block chain-based Iota device authentication mechanism that is both secure and lightweight. A decentralized token-based authentication technique between end-users and block chain-enabled nodes was developed in this study. This approach is intended to be applied in an Iota architecture that is based on block chain technology. In addition to authentication, the authentication strategy that is described in this work allows users to maintain their integrity and adapt if necessary. The findings provide conclusive evidence that the authentication technique that was described may be securely deployed in an Iota environment that is based on Block chain technology. In the future, the effort will concentrate on the administration of the massive quantity of data generated by Iota sensors as opposed to the typical data generated by block chain-based financial transactions. The integrity of the system and its suitability are two additional highly significant aspects of security. In addition, this has been deployed on the Iota platform by using a lightweight block chain design.

Author Contributions

All of the authors agreed on the study's substance. The author has reviewed and approved the final manuscript.

Funding

The authors did not receive any specific funding for this work.

Conflicts of Interest

The authors declare no conflicts of interest.

References:

- [1] G.-G. Zhang and Z. Wan, "Block chain-based Iota security authentication system," in Proc. Int. Conf. Computer, Block chain and Financial Development (CBFD), 2021, pp. 415–418.
- [2] H. A. Hassan, E. E. Hamden, W. El-Safari, M. Shakier, and F. E. Bad El-Sammie, "Intrusion Detection Systems for the Internet of Things: A Survey Study," *Wireless Personal Communications*, vol. 128, no. 4, pp. 2753–2778, 2023.
- [3] G. Gkogkos, C. Patsonakis, A. Dropout, and D. Tovar's, "A DLT-based framework for secure Iota infrastructure in smart communities," *Technology in Society*, vol. 74, Art. No. 102329, 2023.
- [4] S. Abdullah, J. Arched, M. M. Khan, M. Alatza, and K. Selah, "PRISED tangle: A privacy-aware framework for smart healthcare data sharing using IOTA tangle," *Complex & Intelligent Systems*, vol. 9, no. 3, pp. 3023–3041, 2023.
- [5] Y. I. Alzoubi and A. Aljaafreh, "Block chain-Fog Computing Integration Applications: A Systematic Review," *Cybernetics and Information Technologies*, vol. 23, no. 1, pp. 3–37, 2023.
- [6] F. H. Portman, R. K. Das, and G. Sasha, "Block chain-based security aspects in heterogeneous Internet-of-Things networks: A survey," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 10, Art. no. e3741, 2019.
- [7] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Selah, "A user authentication scheme of Iota devices using block chain-enabled fog nodes," in Proc. IEEE/ACS 15th Int. Conf. Computer Systems and Applications (AICCSA), 2018, pp. 1–8.
- [8] J. K. Musher, S. Karla, and J. Amphora, "An efficient block chain based authentication scheme to secure fog enabled Iota devices," in Proc. Indo-Taiwan 2nd Int. Conf. Computing, Analytics and Networks (ICAN), 2020, pp. 75–80.
- [9] Y. Liu, A. Liu, Y. Xia, B. Hub, J. Liu, Q. Wu, and P. Tiara, "A block chain-based cross-domain authentication management system for Iota devices," *IEEE Transactions on Network Science and Engineering*, 2023.
- [10] R. Kumar, D. Jived, A. Aljuhani, A. Jolfaei, P. Kumar, and A. K. M. N. Islam, "Block chain-based authentication and explainable AI for securing consumer Iota applications," *IEEE Transactions on Consumer Electronics*, 2023.
- [11] P. Zhang, Y. Wang, G. S. Aula, A. Tindal, and Y. D. Al-Otaibi, "A block chain-based authentication scheme and secure architecture for Iota-enabled maritime transportation

- systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2322–2331, 2022.
- [12] X. Jiao, M. Lou, H. Wang, J. Sheen, and D. He, "A block chain-assisted privacy-aware authentication scheme for Internet of Medical Things," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 21838–21850, 2022.
- [13] T. Ashen, F. Z. Khan, Z. Irbil, M. Ahmed, R. Alroobaea, A. M. Abash, I. Ali, and M. A. Raze, "Iota devices, user authentication, and data management in a secure, validated manner through the block chain system," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–13, 2022.
- [14] L. Vagan, "Automated security protocol analysis with the AVISPA tool," *Electronic Notes in Theoretical Computer Science*, vol. 155, pp. 61–86, 2006.
- [15] A. Labia, K. Tome, A. Laurite, A. Labe, and S. Martin, "Block chain based trust management mechanism for Iota," in *Proc. IEEE Wireless Communications and Networking Conf. (WCNC)*, 2019, pp. 1–8.
- [16] S. Mali, V. Dedeoglu, S. S. Adhere, and R. Jordan, "Trust chain: Trust management in block chain and Iota supported supply chains," in *Proc. IEEE Int. Conf. Block chain*, 2019, pp. 184–193.
- [17] D. E. Kosice, Y. Imines, A. Bouabdallah, and H. Lachlan, "Decentralized block chain-based trust management protocol for the Internet of Things," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1292–1306, 2020.
- [18] G. Rather, M. Balasaraswathi, K. P. Chandra, S. D. Gupta, and C. S. Boopathi, "A secure Iota sensors communication in Industry 4.0 using block chain technology," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 533–545, 2021.
- [19] S. Latin, Z. Ides, J. Ahmad, L. Zhen, and Z. Zoo, "A block chain-based architecture for secure and trustworthy operations in the Industrial Internet of Things," *Journal of Industrial Information Integration*, vol. 21, Art. No. 100190, 2021.
- [20] A. P. Devi, A. Adhikari, A. R. Demure, N. K. Sabena, A. Sedona and P. C. Biwa's, "Big Data Analytics for Strategic Business Decision-Making: An Empirical Study Across Multi-Sector Organizations," 2026 1st International Conference on AI, Data Science, Cyber Security and Smart Manufacturing for Sustainable Development (ICADCS), Gwalior, India, 2026, pp. 509-513, doi: 10.1109/ICADCS70036.2026.11583166.