International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

A BLOCKCHAIN-BASED APPROACH FOR SECURE AND ECONOMICAL IOT SOFTWARE UPDATE MANAGEMENT

Shiva Kumar. M[1], Karthik. M[2], Nikitha. M[3], Mr. M HariKumar[4]
[1,2,3] UG Scholar, Dept. of IT, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
[4]Assistant Professor, Dept. of IT, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
matamshivakumar7222@gmail.com

Abstract:

The Internet of Things (IoT) market in India is rapidly expanding, with IoT deployments in sectors like healthcare, agriculture, and urban development. IoT devices are being used for patient body temperature monitoring, roadside traffic management, and agricultural climate monitoring. India is expected to reach around 2 billion IoT connections by 2025, indicating the potential of IoT to drive digital transformation across sectors the objective of this work is to design a secure, decentralized, and cost-efficient framework using blockchain and cryptographic techniques to manage software updates for IoT devices, safeguarding against potential threats. Traditional IoT software update systems rely on a centralized server to distribute updates, creating a single point of failure that can disrupt the entire network if the server goes down. So updates are often unencrypted, making them vulnerable to interception or manipulation by hackers Given the significant rise in IoT applications, ensuring secure and tamper-proof software updates is essential. Blockchain provides decentralized, cryptographic mechanisms that can prevent malicious alterations, unauthorized access, and reliance on a single point of failure. Here motivation stems from the need to ensure reliable, accessible, and secure software updates in IoT networks, enabling devices to maintain up-to-date protections against cyber threats. The proposed system leverages blockchain and cryptographic techniques to enhance security and scalability in IoT software updates. Blockchain serves as a secure, decentralized ledger, recording transactions and storing update data hashes to ensure data integrity and prevent tampering. Cipher Policy Attribute Based Encryption (CPABE) is used to encrypt updates, allowing only verified devices on a designated access control list to decrypt them. The Elliptic Curve Digital Signature Algorithm (ECDSA) verifies update authenticity by matching hash values between the sender and receiver, detecting any tampering attempts.

Keywords: Blockchain, Security, Decentralization, Encryption IOT Updates, Smart Contracts, Tampering.

1. INTRODUCTION

This project proposes a blockchain-based approach to secure and manage IoT software updates, ensuring data integrity and preventing tampering. The system offers a decentralized solution that minimizes risks associated with traditional centralized update models. Applications include secure update management for IoT devices in healthcare, smart city infrastructure, and precision agriculture. Traditional IoT software update systems rely on a centralized server for managing updates, which creates a single point of failure. If this server is compromised or becomes inaccessible, it can disrupt the update distribution process, leaving IoT devices vulnerable. These updates are often not encrypted, exposing them to interception and manipulation by cyber attackers, compromising the security and functionality of devices. Payments for these updates are processed using standard web protocols, which are susceptible to attacks, allowing hackers to gain unauthorized access to update systems. Such vulnerabilities endanger data integrity and overall security in mission-critical IoT applications. The rapid increase in IoT adoption across critical sectors makes secure, tamper-proof software updates essential. Blockchain technology offers a decentralized and cryptographic approach, effectively addressing security concerns by ensuring integrity and protecting against unauthorized access. This study is motivated by the need for a reliable, decentralized, and secure update mechanism that enhances the resilience of IoT systems against cyber threats. Using blockchain can prevent reliance on a single point of failure, ensuring that IoT devices consistently maintain up-to-date security features, and stay protected against evolving threats in real-time. these updates are frequently transmitted without encryption, allowing cybercriminals to intercept and alter the data, compromising device security. Payment processes for updates lack robust security, making them vulnerable to unauthorized transactions. This centralized, unprotected structure fails to adequately secure IoT software updates, exposing the network to potential data breaches and system disruptions and scalability issues of traditional IoT software update methods by utilizing blockchain and cryptographic techniques. Blockchain technology functions as a decentralized, immutable ledger that records transactions and stores update hashes, ensuring data integrity and preventing tampering. To further secure the system, Cipher Policy Attribute-Based Encryption (CPABE) is employed, enabling encrypted updates that only verified devices on a designated access list can decrypt. Additionally, the Elliptic Curve Digital Signature Algorithm (ECDSA) provides authenticity verification by matching hash values between the sender and receiver, safeguarding against tampering. Removing single points of failure, blockchain technology offers resilience against network-wide outages, making this system an essential addition to India's growing IoT infrastructure. This solution is invaluable for safeguarding public safety, privacy, and functionality in real-world IoT applications.

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

2. LITERATURE SURVEY

Yousef nezhad et al. proposed a framework that uses packet header information, sensor measurement and statistical feature sets as features for classifying and identifying IoT devices. Several machine learning methods such as RF, Support Vector Machine (SVM), and Logistic Regression (LR) were used for training the model. The experimental results show that the accuracy is better for the measurement-header model. Marchal et al. proposed a system named AuDI for fingerprinting device types in an IoT system. In the proposed system, no prior information is required, and information from periodic communication traffic was used for device identification using an unsupervised machine learning method. The experimental result shows that the proposed system can identify devices with 98.2% accuracy. Hamad et al. proposed a passive device fingerprinting technique for IoT systems. In the proposed system, the fingerprint is created from features selected using both packet headers and payload information. A supervised machine learning method is used for detecting behavioral changes in devices and hence identifying a rogue device for further monitoring. The proposed technique can also identify devices from the same model and vendor with 90.3% accuracy. Yin et al. proposed IoT ETEI, a deep learning-based automatic end- to-end IoT device identification method. The proposed method is based on CNN+ Bi LSTM and uses spatial and temporal features extracted from traffic to identify devices. The author argues that since the proposed method does not require any prior knowledge for feature engineering, it is efficient in terms of low overhead. The performance of the proposed model was evaluated using two publicly available data sets (UNSW smart home traffic dataset containing 22 IoT devices and Your Things smart home traffic dataset containing 17 IoT devices) and the results show that the proposed method achieves accuracy rates of 99.91% and 99.68%, respectively. Miettinen et al. proposed a system named IoT SENTINEL to identify the types of IP based IoT devices being connected to a network. In this work, the device type is defined as a combination of device model and software version, and device fingerprinting was based on passive observation of network traffic. Twenty-three packet features were used for feature engineering, and all of these features were extracted from encrypted traffic (which does not require to rely on packet payload). The author argues that the proposed system has low overhead and can identify devices effectively. Gong et al. proposed a blockchain-based identity authentication framework for IoT devices. In the proposed system blockchain is used to store device identity information, and a Blockchain of Things (B CoT) Gateway was proposed for recording authentication transactions. This work uses device traffic flow for the device recognition model. Wang, D. et al performance of the proposed model was evaluated using a public dataset and the results show that the proposed system can recognize devices with an accuracy rate of over 95%. For device management, blockchain is used to identify and register IoT devices in a smart grid . Dorri.A.et al. Multiple consensus algorithms are also studied and compared when employed in the proposed system. Numerous and identification based on the transaction history in blockchain-based IoT applications, an obfuscation-based technique is proposed. As IoT devices generate transactions based on a time pattern so different timestamp related obfuscation methods are used to break the pattern and results show a significant reduction in informed and blind attacks. Mohanta, B .et al A distributed authentication system using blockchain is proposed that provides a means to login to any application that supports that authentication system. A smart contract in the authentication blockchain application stores the user ID and user wallet address at the start. This authentication step may need a few minutes to complete when Ethereum is used as a blockchain platform due to the transaction rate.

The results showed that the proposed system could be very effective against some attacks like man in the middle, impersonation, replay and DoS. Shukla, S. et al. A fog computing and blockchain-based three tier architecture is proposed that provides services for transactions and transmission near the edge in a secure manner. The proposed solution is designed for data sensitive healthcare IoT applications to provide security, reliability and authenticity. The results showed that the proposed system could effectively detect malicious nodes and is reliable. The data processing at the edge of the IoT network improves throughput and execution time. Yang, H. et al For Industrial IoT (IIoT), a trusted anonymous access architecture based on a private blockchain is proposed where three different types of Software Defined Network (SDN) controllers are used for providing trusted access. To provide a balanced trade-off among credibility, confidentiality and efficiency a special module is designed in the system that shows good results in case of heavy traffic load as compared to other approaches. Maram, D.et al mentioned approaches used machine learning for device identification and fingerprinting using network traffic information or RF for feature engineering. Sensors and hubs are light weight devices and any such approach may produce a lot of overhead. Our protocol introduces minimum overhead in terms of storage and process-ing at sensors and hubs. Using the timing information the hub can identify each sensor individually and authenticate the data sent by that sensor. The existing research mentioned above that used blockchain for device identification mostly requires blockchain to save device information. Our approach focuses on using blockchain to provide the validity of the sensor data stored in the database and no device information is stored on the blockchain. Abosta et al. have proposed a decentralized user identity management system that provides accountability and Sybil attack resistance while being compatible with legacy web services. Users are able to recover their keys using existing online accounts using other online systems. The system has two main modules: an identity system and a key recovery system that relies on a decentralized set of nodes. Li. M et al. proposed a blockchain-based Vehicular Digital Forensics (VDF) scheme named Eunomia to provide a secure mechanism to share data for forensic purposes with the ability to track malicious users. Even though both of the above mentioned systems provide a number of novel features, they have not been evaluated in the context of device identification.

3. PROPOSED METHODOLOGY

The increasing adoption of Internet of Things (IoT) devices across various industries, such as healthcare, smart homes, industrial automation, and transportation, has raised significant concerns regarding software update security, reliability, and efficiency. Traditional software update management systems rely on centralized servers, making them vulnerable to cyberattacks, data breaches, and operational failures. Additionally, these systems often suffer from high infrastructure costs, slow update propagation, and a lack of transparency, making it difficult to ensure the integrity and authenticity of software updates. To address these challenges, the project proposes a blockchain-based IoT software update management system that leverages decentralized ledger technology, smart contracts, cryptographic verification, and distributed storage to ensure a secure, transparent, and cost-efficient software update process for IoT devices. Future enhancements include integrating adaptive learning techniques and real-time implementation for broader applicability. Additionally, we explore the potential integration of cloud-based processing to enhance scalability and enable large-scale data handling. The implementation of a feedback-driven learning mechanism is also considered to continuously refine the model based on real-world performance. Furthermore, the proposed methodology is designed to be adaptable for various application domains, ensuring versatility in practical scenarios. Emphasis is placed on optimizing energy efficiency in computational processes, making the approach suitable for resource-constrained environments.

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

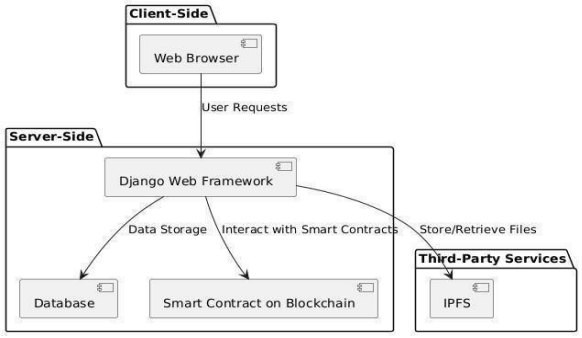


Figure 1: Block diagram.

Key Components:

Secure and Transparent Update Distribution: Leverage blockchain's immutable ledger to store and verify update records, preventing unauthorized changes or attacks.

Smart Contract-Driven Update Management: Use Ethereum smart contracts to automate update verification, approval, and deployment processes.

Efficient Update Storage and Retrieval: Store firmware updates using decentralized file systems like IPFS (Inter Planetary File System) and provide secure retrieval mechanisms for IoT devices.

Cryptographic Verification: Implement digital signatures and hash-based verification to ensure firmware authenticity before deployment.

Automated IoT Update Client: Design a lightweight update client for IoT devices to interact with the Django-based backend and retrieve secure software updates.

System Architecture with Django:

Django Web Framework: Provides a secure and scalable backend for managing software updates. Implements user authentication, role-based access control, and a dashboard for update tracking**.**

Blockchain Network: Stores update transactions immutably on the blockchain for transparency. Uses smart contracts to enforce update rules and automate verification.

Decentralized Storage: Stores firmware updates in a distributed, tamper-proof environment. Reduces network congestion and cloud storage costs.

Django REST API for IoT Devices: IoT devices fetch available software updates through a RESTful API provided by Django. Devices verify update integrity using blockchain- based hash verification**.**

Smart Contract Integration with Django: Uses Web3.py to interact with Ethereum smart contracts from the Django backend. Ensures updates are deployed only after blockchain- based authentication.

Applications:

Healthcare: Ensures secure updates for patient-monitoring devices, protecting sensitive health data and ensuring uninterrupted operation of critical medical equipment.

Smart Cities: Helps secure updates for infrastructure such as traffic control systems and environmental sensors, enhancing public safety and efficiency.

Agriculture: Maintains secure communication between IoT devices monitoring soil conditions and climate, ensuring accurate data collection for crop management.

Healthcare: The decentralized architecture enhances security by preventing unauthorized modifications, ensuring patient safety, and complying with healthcare regulations. By eliminating single points of failure, blockchain reduces cyberattack risks and enhances the reliability of medical devices.

Advertiser Insights: Advertisers targeting young audiences can analyze sentiment data to tailor ads that align with the positive sentiments expressed

Advantages:

Enhanced Security:

Blockchain's decentralized nature eliminates a single point of failure, reducing the risk of cyberattacks. Handles Social.

Tamper-Proof Updates:

Blockchain's immutability ensures that software updates cannot be altered once they are recorded, reducing the risk of malicious updates.

Cost-Effective and Scalable:

The use of Interplanetary File System (IPFS) reduces the need for large centralized storage, cutting down on infrastructure costs.

Decentralized Control:

IoT devices can securely receive updates without relying on a central authority, making the system more resilient to server failures.

4. EXPERIMENTAL ANALYSIS

Figure 1 shows that the screen click on 'Register Here' link to get below signup screen and then add manufacturer and owner records.

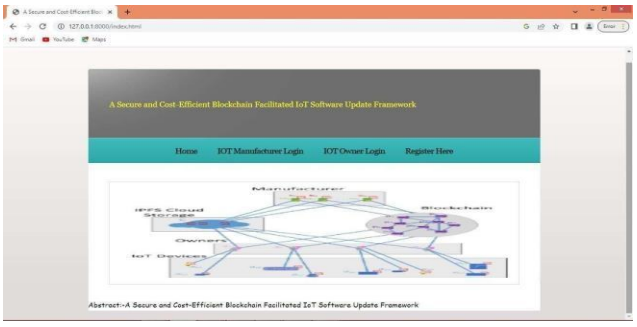


Figure 1: Home Page

Figure 2 shows screen click on 'Register Here' link to get below signup screen and then add manufacturer and owner records

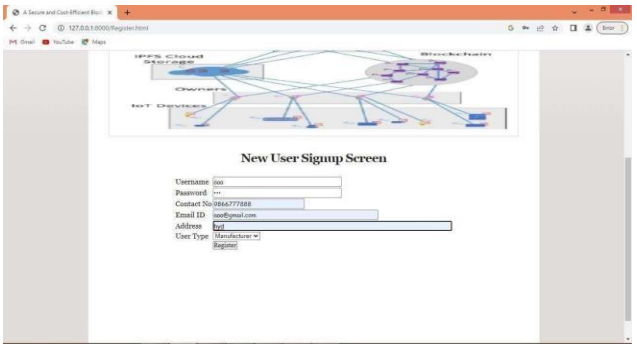


Figure 2: New User Signup

In above screen adding one user as manufacturer and then click 'Register' button to add user details to Blockchain and get below page. user details added and now add owner details.

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

In above screen manufacturer is login and after login will get below page.

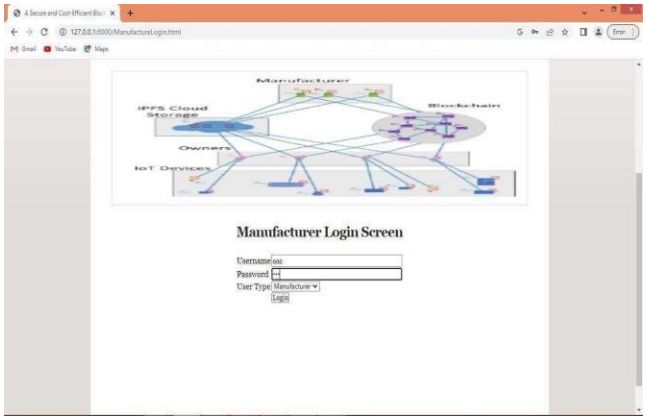


Figure 3: Login page.

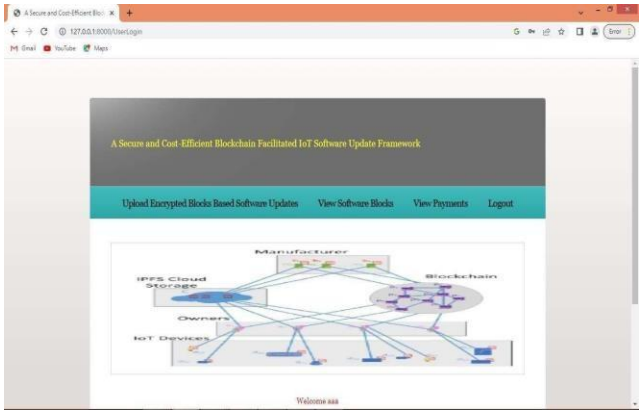


Figure 4: Upload Encrypted Blocks Based Software.

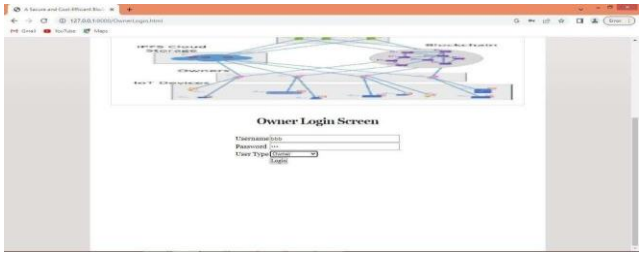
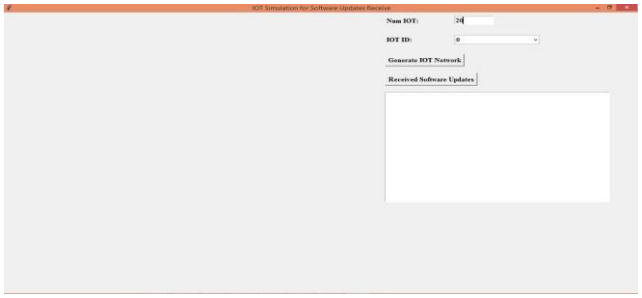


Figure 5: Owner Login Screen
Figure 6: Generating IOT Network



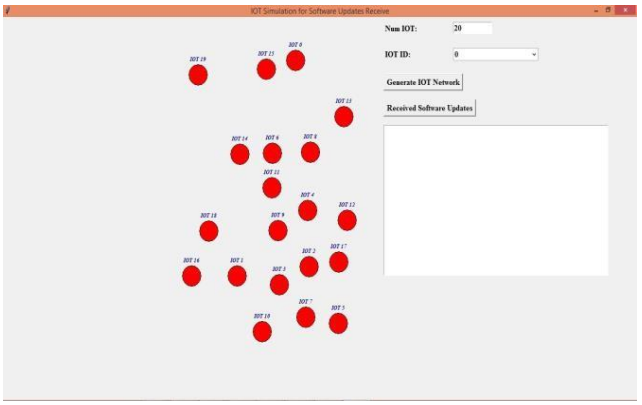


Figure 7: 22 Downloading Software updates for IOT

Figure 8 shows all red colour circles are consider as IOT nodes and are placed at different location and now click on 'Received Software Updates' button to download and update software only for those IOT's purchased by owner.

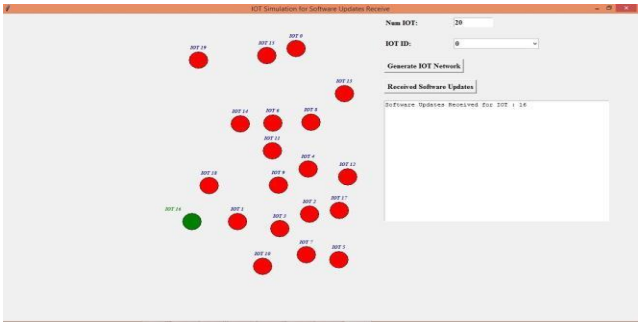


Figure 8: Updates purchased for IOT

Figure 8 shows that we screen we can see the IOT for which IOT owner purchase updates will receive and we can its colour to green to indicate as its receiving updates.

5. CONCLUSION

The Blockchain-Based IoT Software Update Management System provides a secure, decentralized, and transparent approach to firmware updates for IoT devices. By leveraging blockchain's immutability, the system prevents unauthorized modifications, ensuring that only verified firmware updates reach IoT devices. The integration of Django for backend operations and smart contracts for update verification enhances system reliability and security. Additionally, the use of cryptographic hashing and digital signatures ensures the integrity and authenticity of each update, mitigating the risk of malware injection. The system also offers real-time monitoring, role-based access control, and automatic anomaly detection, making it a robust solution for organizations managing large-scale IoT deployments. This approach eliminates the vulnerabilities of traditional update mechanisms, reducing the risks associated with cyberattacks, device failures, and unauthorized firmware alterations.

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

REFERENCES

[1] Yousefnezhad, N.; Malhi, A.; Främling, K. Automated IoT Device Identification Based on Full Packet Information Using Real-Time Network Traffic. Sensors 2023,21, 2660. Zheng, B.; Niiya, M.; Warschauer, M. Wikis and collaborative learning in higher education. Technol. Pedagog. Educ. 2015, 24, 357–374. [Google Scholar] [CrossRef]

[2] Marchal, S.; Miettinen, M.; Nguyen, T.D.; Sadeghi, A.R.; Asokan, N. AuDI: Toward Autonomous IoT Device-Type Identification Using Periodic Communication. IEEE J. Sel. Areas Commun. 2023,37, 1402–1412.

[3] Hamad, S.A.; Zhang, W.E.; Sheng, Q.Z.; Nepal, S. IoT Device Identification via Network-Flow Based Fingerprinting and Learning. In Proceedings of the 2022 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 5–8 August 2022.

[4] Yin, F.; Yang, L.; Wang, Y.; Dai, J. IoT ETEI: End-to-End IoT Device Identification Method. In Proceedings of the 2022 IEEE Conference on Dependable and Secure Computing (DSC), Aizuwakamatsu, Japan, 30 January–2 February 2022; pp. 1–8.

[5] Miettinen, M.; Marchal, S.; Hafeez, I.; Asokan, N.; Sadeghi, A.R.; Tarkoma, S. IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT. In Proceedings of the 2022 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2022; pp. 2177–2184.

[6] Gong, L.; Alghazzawi, D.M.; Cheng, L. BCoT sentry: A blockchain-based identity authentication framework for IoT devices. Information 2022,12, 203.

[7] Wang, D.; Wang, H.; Fu, Y. Blockchain-based IoT device identification and management in 5G smart grid. EURASIP J. Wirel. Commun. Netw. 2022, 125.

[8] Dorri, A.; Roulin, C.; Pal, S.; Baalbaki, S.; Jurdak, R.; Kanhere, S. Device Identification in Blockchain-Based Internet of Things. IEEE Internet Things J. 2022, Early Access.

[9] Mohanta, B.K.; Sahoo, A.; Patel, S.; Panda, S.S.; Jena, D.; Gountia, D. DecAuth: Decentralized Authentication Scheme for IoT Device Using Ethereum Blockchain. In Proceedings of the TENCON 2019—2021 IEEE Region 10 Conference (TENCON), Kochi, India, 17–20 October 2021; pp. 558–563.

[10] Shukla, S.; Thakur, S.; Hussain, S.; Breslin, J.G.; Jameel, S.M. Identification and Authentication in Healthcare Internet-of-Things Using Integrated Fog Computing Based Blockchain Model. Internet Things 2021,15, 100422.

[11] Yang, H.; Bao, B.; Li, C.; Yao, Q.; Yu, A.; Zhang, J.; Ji, Y. Blockchain-Enabled Tripartite Anonymous Identification Trusted Service Provisioning in Industrial IoT. IEEE Internet Things J. 2020,9, 2419–2431.

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

[12] Maram, D.; Malvai, H.; Zhang, F.; Jean-Louis, N.; Frolov, A.; Kell, T.; Lobban, T.; Moy, C.; Juels, A.; Miller, A. Candid: Can-do decentralized identity with legacy compatibility, sybil-resistance, and accountability. In Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 24–27 May 2020; pp. 1348–1366.

[13] Abosata, N.; Al-Rubaye, S.; Inalhan, G.; mmanouilidis, C. Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. Sensors 2019,21, 3654.

[14] Li, M.; Chen, Y.; Lal, C.; Conti, M.; Alazab, M.; Hu, D. Eunomia: Anonymous and secure vehicular digital forensics based on blockchain. IEEE Trans. Dependable Secur 2019.