A BLOCKCHAIN BASED SECURE AND EFFICIENT VALIDATION SYSTEM FOR DIGITAL CERTIFICATES

C.RASHMI[1], G. ARCHANA[2], K. RASHMIKA[2], K. SPANDANA[2], CH. MANASA[2]

[1]Assistant Professor, Department of Information Technology, Mallareddy Engineering College for Women, (UGC-Autonomous), Hyderabad, India, rrashmi.cigiri@gmail.com.

[2]Student, Department of Information Technology, Mallareddy Engineering College for Women, (UGC-Autonomous), Hyderabad, India.

Abstract

Certificate forgery has been a persistent issue across various industries, causing concerns in education, professional certifications, and legal documentation. In the past, verifying certificates was a manual and time-consuming process, involving physical examination of paper-based documents and cross-referencing with centralized databases or authorities. Unfortunately, this approach lacked transparency, was slow, and provided opportunities for fraudulent activities. Moreover, the vulnerability of traditional paper certificates to tampering and counterfeiting raised doubts about their authenticity and reliability. Thankfully, recent technological advancements have opened up a promising solution to combat certificate forgery by utilizing blockchain technology for certificate verification. Therefore, this project proposes an innovative approach to tackle this problem head-on. By harnessing the capabilities of blockchain, this work aims to create a robust and tamper-resistant certificate verification platform. Blockchain technology offers a decentralized and immutable way of storing and managing data, making it an ideal candidate to revolutionize certificate verification. With this system, the entire process becomes more efficient and secure. Each certificate issuance is recorded in a tamper-proof manner, complete with a timestamp, which virtually eliminates the possibility of altering or deleting information. The decentralized nature of blockchain removes the need for reliance on a central authority, reducing the risk of data manipulation and fostering trust in the verification process. This means that certificates can be verified without the involvement of a single controlling entity, making the system more reliable and transparent. In addition, the proposed system addresses the challenges associated with certificate forgery and offers a secure, efficient, and trustworthy solution. By leveraging blockchain technology, this proposed system can revolutionize current practices and ensure that certificates hold their true value and authenticity, thus maintaining the integrity of various industries plagued by this long-standing problem.

1. Introduction

A blockchain-based secure and efficient validation system for digital certificates represents a groundbreaking solution to address the challenges associated with certificate verification, authentication, and fraud prevention. This system leverages the inherent characteristics of blockchain technology, such as immutability, transparency, and decentralization, to revolutionize the way digital certificates are managed and verified.At its core, this system operates by storing digital certificate data on a blockchain ledger, ensuring that once a certificate is issued, it cannot be tampered with or altered. Each certificate is represented as a unique digital token on the blockchain, making it easy to verify its authenticity and origin. Furthermore, the decentralized nature of blockchain ensures that there is no single point of failure, reducing the risk of data breaches and unauthorized access.Efficiency is a key feature of this system. Traditional methods of certificate validation can be time-consuming and susceptible to errors. With blockchain, verification becomes instantaneous and highly reliable. Institutions, employers, and individuals can quickly confirm the legitimacy of a certificate by accessing the blockchain, eliminating the need for time-consuming manual checks.Security is

paramount in this system. The cryptographic nature of blockchain technology ensures that data is encrypted and protected against unauthorized access. This safeguards sensitive certificate information from potential hackers and fraudulent activity. Moreover, the transparency of blockchain allows stakeholders to track the entire history of a certificate, from issuance to validation, enhancing trust and accountability.

2. Literature Survey

The proliferation of industrial IoT applications and networking services has facilitated a tremendous increase in the number of connected devices. These application devices can capture real-time industrial data with a dedicated sensor unit [1]. Industrial advancement and technological guidance are behind this shift in how systems interact with physical and logical things. A centralized architecture is used to communicate real-time industrial data and evaluate the critical components of IoT, including identity management [2]. A single failure point is feasible due to this common technique [3]. A significant issue with the Internet of Things (IoT) is the difficulty in maintaining and managing many connected devices [4]. A system of networks can talk interactively through adaptive self-configuration. IoT applications can be commercialized over the 6G network. A fundamental component of the IoT, the wireless sensor network (WSN) gathers and transmits physical data using various heterogeneous models [5]. Data security is a major concern of IoT systems because they are built by connecting many IoT devices [6]. Data generated by these devices are stored in the cloud and transmitted across various networks. A cyber-attack on a smart healthcare system can substantially impact the system's ability to produce and supply electricity. In addition to financial and other types of damage, cyber-attacks on smart healthcare can cause operational failures, power outages, the theft of critical data, and complete security breaches [7]. Cyber experts face difficulties keeping tabs on everything that passes via a smart grid and recognizing potential threats and attacks. Even though machine learning has become an essential part of cybersecurity, the problem is that this field requires distinct approaches and theoretical viewpoints to handle the enormous volume of data generated and transported across numerous networks in a smart grid [8]. The attacks and threats that could be launched against this proof-of-concept environment are being determined using threat modeling. Several potential threats have been tested, including detection, tampering, repudiation, information leakage, denial of service (DoS), and extended privilege (EoP). Each of the risks and the security elements associated with them are addressed using STRIDE. STRIDE is a typical threat modeling technique for finding and classifying attack vectors [9]. Using the well-known industrial framework MITRE ATTCK, researchers can detect threats disguised as tactics, techniques, and procedures (TTP) [10].

Based on the above, blockchain technology could be one of the main solutions for IoT security issues [11]. A blockchain provides a decentralized system using a consensus mechanism and smart contracts [12]. Smart contracts are the protocols that trigger the blockchain to act according to a particular activity or situation [13]. Blockchains can be categorized into three classes: private, public, and hybrid public blockchain technology. The main feature of a blockchain is to provide security and only keep records and transactions within a single organization. A public blockchain provides access to the public using a public API. Moreover, such a model interacts with external networks such as gateway networks or cloud outsourcing. A hybrid blockchain is also called a consortium blockchain, which provides features of both a private and public blockchain. Blockchain technology can be used to build trust and monitor node activity in IoT networks. It is challenging to integrate a blockchain into IoT applications due to its high power consumption and job outsourcing [14]. Several blockchain-based Internet of Things (IoT) applications have recently been created to address these concerns. These blocks can be used to delete old transactions and blocks from the blockchain without jeopardizing

security. Pan et al. [15] created an IoT resource management prototype using blockchain technology and smart contracts to securely record all IoT transactions [15]. Deploying smart contracts involves evaluating the source code, bytes of code, and execution histories. This is how we test our computer traffic analysis deployment scenario. Ali et al. [16] investigated blockchain technology and smart contract applications in cloud storage. Tam et al. utilize a pay-as-you-go car business model. This technology's strengths are traceability and tamper-proof characteristics. Ali et al. [17] created a blockchain-based publisher–subscriber model. They designed their solution to ensure data integrity in real-time IoT processing by balancing computational resources and workload. Liu et al. delegated computationally intensive POW mining tasks to nearby edge servers in blockchain-enabled mobile IoT systems [18]. Chen et al. conducted additional research. Securing biometric data for patient authentication is a common issue. In particular, finger vein biometric data has been studied extensively. A strong verification mechanism with high levels of reliability, privacy, and security is required to better secure these data. Also, biometric data are difficult to replace, and any leakage of biometric data exposes users to serious threats, such as replay attacks employing stolen biometric data. This research offers a unique verification secure framework based on triplex blockchain-based particle swarm optimization (PSO)-advanced encryption standard (AES) approaches in medical systems for patient authentication. The discussion has three stages. First presented is a new hybrid model pattern based on RFID and finger vein biometrics to boost randomness. It proposes a new merge method that combines RFID and finger vein characteristics in a random pattern. Second, the suggested verification safe framework is based on the CIA standard for telemedicine authentication using AES encryption, blockchain technology, and PSO in steganography [19]. Finally, the proposed secure verification architecture was validated and evaluated [20]. The combination of WSN functional activities with 6G network topologies allows us to test a wide range of IoT application deployment models. Many IoT devices collect data using IPV6 across low-power wireless personal area networks and wearables (6LoWPAN) [21,22]. We were able to keep user data confidential with the help of AKA [23]. Companies that use public cloud services and large-scale data storage systems have long prioritized client data protection [24].

3. Proposed System Design

The process flows in the system are captured in the activity diagram. Similar to a state diagram, an activity diagram also consists of activities, actions, transitions, initial and final states, and guard conditions.

3.1 Blockchain

Blockchain is a decentralized, digital ledger technology that is used to record and store data in a secure and transparent manner. It is a distributed ledger, meaning that it is maintained by a network of computers, rather than being controlled by a single entity. Each block in the chain contains a set of transactions, and once a block is added to the chain, it cannot be altered or deleted. This makes blockchain an immutable and tamper-resistant technology that is particularly well-suited for storing and transmitting sensitive data.Blockchain technology is perhaps best known for its use in cryptocurrencies like Bitcoin and Ethereum, but it has a wide range of other potential applications as well. These include supply chain management, identity verification, voting systems, and more. The decentralized nature of blockchain means that it has the potential to disrupt a variety of industries and business models by enabling trust and transparency in transactions and data exchange. Blockchain is a decentralized, digital ledger technology that is used to record and store data in a secure and transparent manner. It is a distributed ledger, meaning that it is maintained by a network of computers, rather than being controlled by a single entity. Each block in the chain contains a set of transactions, and once a block is added to the chain, it cannot be altered or deleted. This makes blockchain an

immutable and tamper-resistant technology that is particularly well-suited for storing and transmitting sensitive data.Blockchain technology is perhaps best known for its use in cryptocurrencies like Bitcoin and Ethereum, but it has a wide range of other potential applications as well. These include supply chain management, identity verification, voting systems, and more. The decentralized nature of blockchain means that it has the potential to disrupt a variety of industries and business models by enabling trust and transparency in transactions and data exchange.

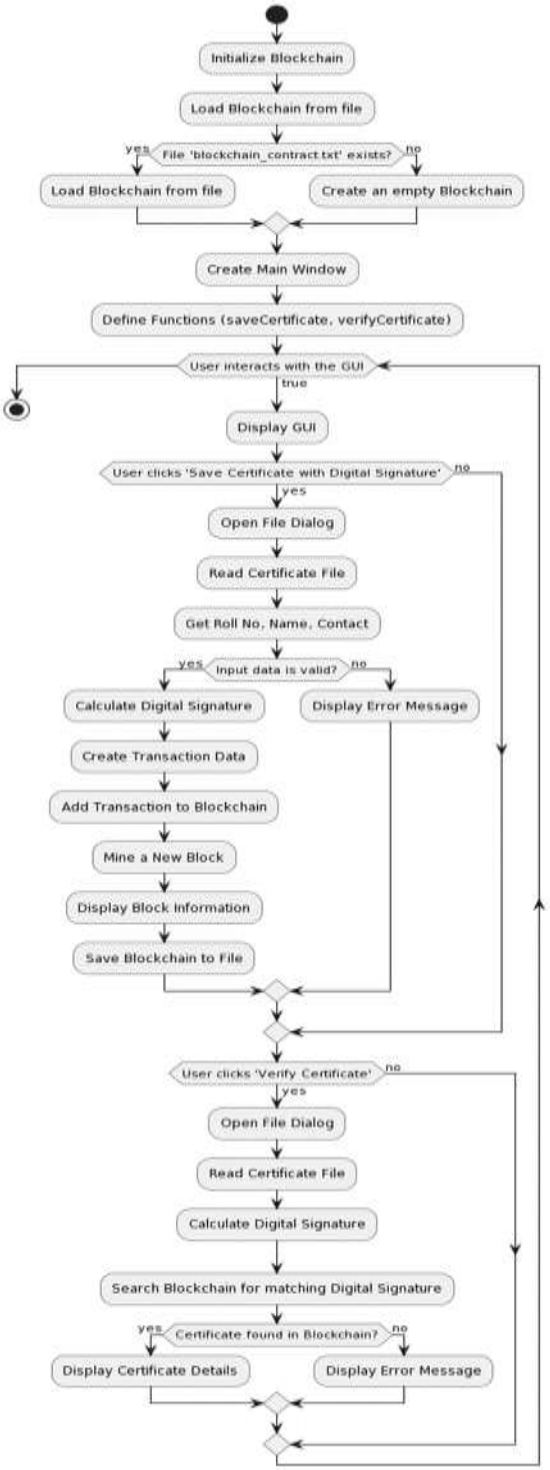

Figure 1. Proposed system design.

4. Results and description

Figure 2 shows the initial state of the graphical user interface (GUI) when the application is launched.

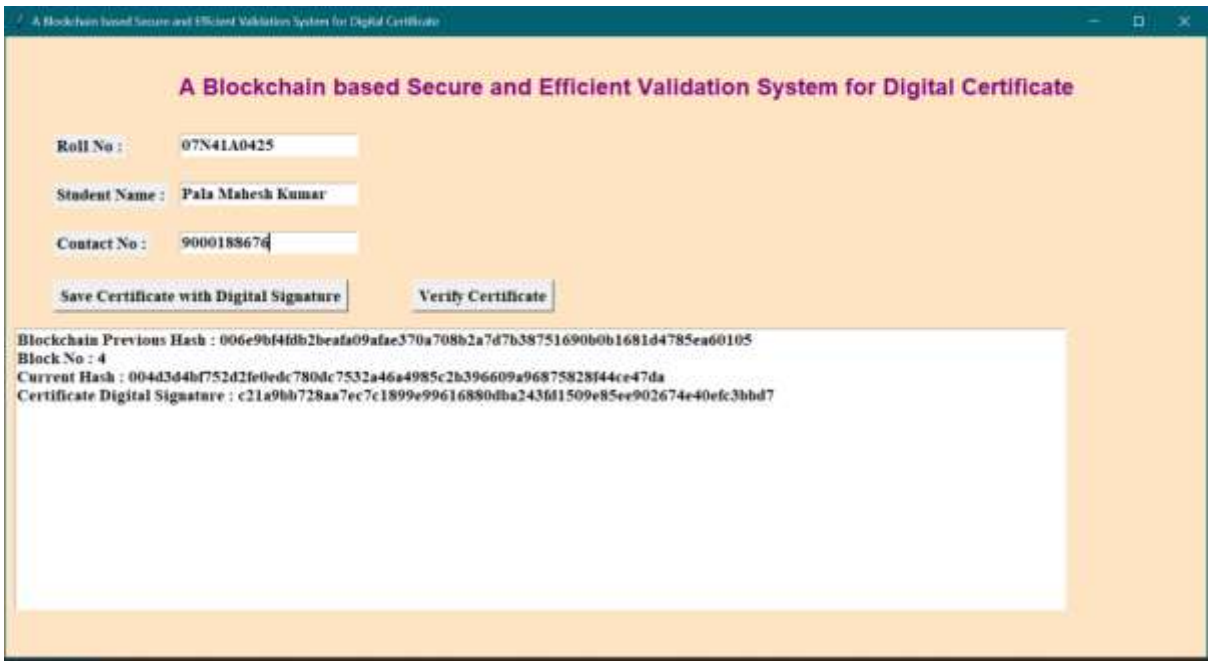

Figure. 3: GUI application after entering the details of student with roll number, student name, and contact information.

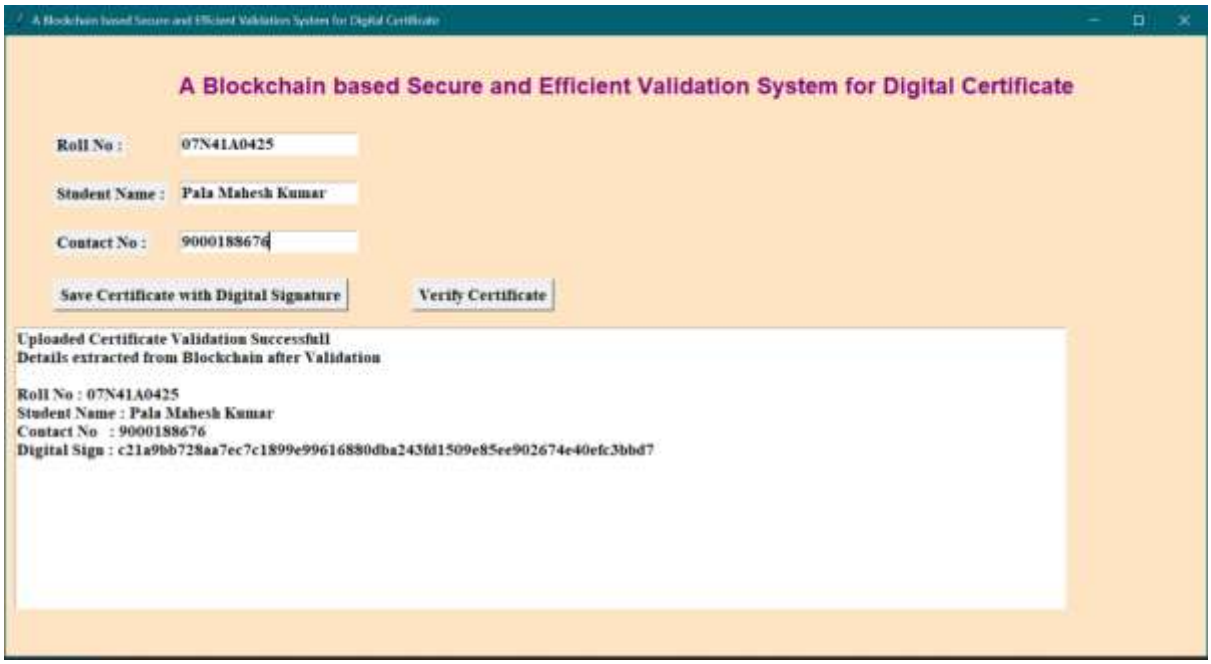

Figure. 4: Illustration of proposed GUI application after storing the certificate with student entry details.

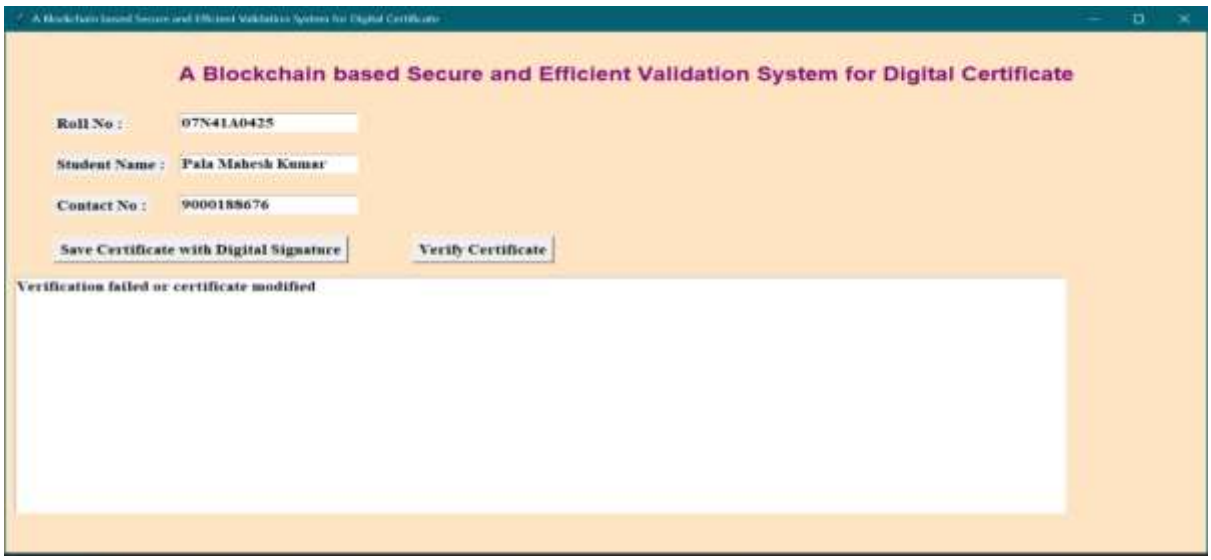

Figure. 5: Checking the certificate verification with test template as input and displaying the validation is successfully verified with student enrolment.

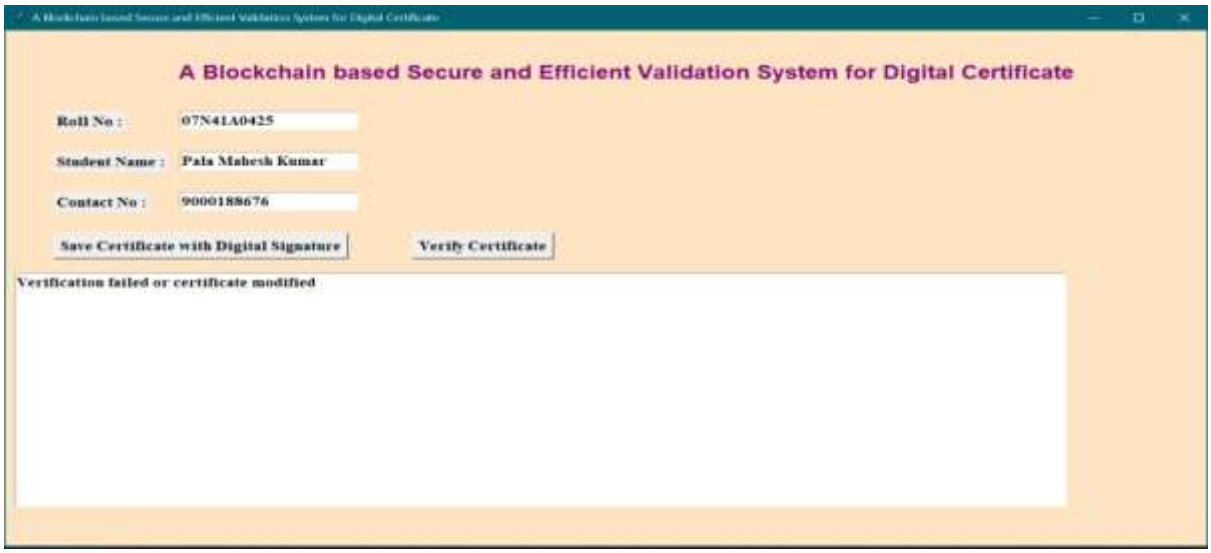

Figure. 6: GUI application with verification of certificate is failed or the certificate is modified.

5. Conclusion

In conclusion, the implementation of blockchain technology in certificate verification holds immense potential for combating the persistent problem of certificate forgery across various industries. By offering a decentralized, tamper-resistant, and transparent platform, this innovative approach addresses the limitations of traditional verification methods. The immutability of blockchain ensures that certificate records remain secure and unalterable, thereby enhancing their credibility and authenticity. Additionally, the elimination of central authorities reduces the risk of data manipulation and fosters trust in the verification process. However, to fully realize the benefits of blockchain-powered certificate verification, several challenges must be overcome. These include ensuring widespread adoption of the technology, addressing scalability issues, and developing user-friendly interfaces for individuals and institutions.

References

[1]. Siam, A.I.; Almaiah, M.A.; Al-Zahrani, A.; Elazm, A.A.; El Banby, G.M.; El-Shafai, W.; El-Samie, F.E.A.; El-Bahnasawy, N.A. Secure Health Monitoring Communication Systems Based on IoT and Cloud Computing for Medical Emergency Applications. Comput. Intell. Neurosci. 2021, 2021, 8016525.

[2]. Ali, A.; Pasha, M.F.; Fang, O.H.; Khan, R.; Almaiah, M.A.; KAl Hwaitat, A. Big data based smart blockchain for information retrieval in privacy-preserving healthcare system. In Big Data Intelligence for Smart Applications; Springer International Publishing: Cham, Switzerland, 2022; pp. 279–296. [Google Scholar]

[3]. Altulaihan, E.; Almaiah, M.A.; Aljughaiman, A. Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions. Electronics 2022, 11, 3330. [Google Scholar]

[4]. Hasnain, M.; Pasha, M.F.; Ghani, I.; Mehboob, B.; Imran, M.; Ali, A. Benchmark Dataset Selection of Web Services Technologies: A Factor Analysis; IEEE Access: Piscataway, NJ, USA, 2020; Volume 8, pp. 53649–53665. [Google Scholar]

[5]. Ali, A.; Rahim, H.A.; Pasha, M.F.; Dowsley, R.; Masud, M.; Ali, J.; Baz, M. Security, Privacy, and Reliability in Digital Healthcare Systems Using Blockchain. Electronics 2021, 10, 2034. [Google Scholar]

[6]. Almaiah, M.A.; Hajjej, F.; Ali, A.; Pasha, M.F.; Almomani, O. An AI-Enabled Hybrid Lightweight Authentication Model for Digital Healthcare Using Industrial Internet of Things Cyber-Physical Systems. Sensors 2022, 22, 1448. [Google Scholar]

[7]. Yazdinejad, A.; Dehghantanha, A.; Parizi, R.M.; Srivastava, G.; Karimipour, H. Secure Intelligent Fuzzy Blockchain Framework: Effective Threat Detection in IoT Networks. Comput. Ind. 2023, 144, 103801.

[8]. Hameed, K.; Ali, A.; Naqvi, M.H.; Jabbar, M.; Junaid, M.; Haider, A. Resource management in operating systems-a survey of scheduling algorithms. In Proceedings of the International Conference on Innovative Computing (ICIC), Lanzhou, China, 2–5 August 2016; Volume 1. [Google Scholar]

[9]. Singh, H.; Ahmed, Z.; Khare, M.D.; Bhuvana, J. An IoT and Blockchain-Based Secure Medical Care Framework Using Deep Learning and Nature-Inspired Algorithms. Int. J. Intell. Syst. Appl. Eng. 2023, 11, 183–191. [Google Scholar]

[10]. Kim, H.; Kim, S.-H.; Hwang, J.Y.; Seo, C. Efficient Privacy-Preserving Machine Learning for Blockchain Network. IEEE Access 2019, 7, 136481–136495. [Google Scholar]

[11]. Sharma, P.; Namasudra, S.; Crespo, R.G.; Parra-Fuente, J.; Trivedi, M.C. EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. Inf. Sci. 2023, 629, 703–718. [Google Scholar]

[12]. Almadani, M.S.; Alotaibi, S.; Alsobhi, H.; Hussain, O.K.; Hussain, F.K. Blockchain-based multi-factor authentication: A systematic literature review. Internet Things 2023, 23, 100844.

[13]. Kumar, P.; Kumar, R.; Gupta, G.P.; Tripathi, R.; Jolfaei, A.; Islam, A.N. A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. J. Parallel Distrib. Comput. 2023, 172, 69–83.

[14]. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Choo, K.-K.R. P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking. Comput. Secur. 2020, 88, 101629.

[15]. Sharma, P.C.; Mahmood, R.; Raja, H.; Yadav, N.S.; Gupta, B.B.; Arya, V. Secure authentication and privacy-preserving blockchain for industrial internet of things. Comput. Electr. Eng. 2023, 108, 108703.

[16]. Jiang, S.; Cao, J.; Wu, H.; Yang, Y. Fairness-Based Packing of Industrial IoT Data in Permissioned Blockchains. IEEE Trans. Ind. Inform. 2020, 17, 7639–7649.

[17]. Bordel, B.; Alcarria, R.; Robles, T. A Blockchain Ledger for Securing Isolated Ambient Intelligence Deployments Using Reputation and Information Theory Metrics; Wireless Networks: New York, NY, USA, 2023; pp. 1–7. [Google Scholar]

[18]. Selvarajan, S.; Srivastava, G.; Khadidos, A.O.; Khadidos, A.O.; Baza, M.; Alshehri, A.; Lin, J.C.-W. An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. J. Cloud Comput. 2023, 12, 38.

[19]. Lacity, M.C. Addressing Key Challenges to Making Enterprise Blockchain Applications a Reality. J. Mis. Q. Exec. 2018, 17, 3. [Google Scholar]

[20]. Sengupta, J.; Ruj, S.; Das Bit, S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. J. Netw. Comput. Appl. 2020, 149, 102481.

[21]. Pajooh, H.; Rashid, M.; Alam, F.; Demidenko, S. Multi-Layer Blockchain-Based Security Architecture for Internet of Things. Sensors 2021, 21, 772.

[22]. Peng, C.; Wu, C.; Gao, L.; Zhang, J.; Yau, K.-L.A.; Ji, Y. Blockchain for Vehicular Internet of Things: Recent Advances and Open Issues. Sensors 2020, 20, 5079.

[23]. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? IEEE Cloud Comput. 2018, 5, 31–37.

[24]. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Inform. J. 2018, 25, 1398–1411.

[25]. Kim, T.M.; Lee, S.-J.; Chang, D.-J.; Koo, J.; Kim, T.; Yoon, K.-H.; Choi, I.-Y. DynamiChain: Development of Medical Blockchain Ecosystem Based on Dynamic Consent System. Appl. Sci. 2021, 11, 1612.