International Journal of Research in Engineering and Management Sciences (IJREMS)
E-ISSN: 3107-7439

Research Article
VOL.: 1, Issue: 1, June 2025

Enhancing IoT Security with Blockchain Technology: A Scalable Solution for Device Authentication

[1]Dr. Venkateswarlu B.

*[*1]Assistant Professor, Department of Computer Science and Engineering,*
Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Andhra Pradesh, India
Email: bvenki289@gmail.com
Orcid ID: https://orcid.org/0009-0006-6171-1238

ABSTRACT:

Internet of Things (IoT) has overwhelmed the industries creating interdependence among the devices, automation of the system, and data sharing. Security issues have however come into place and in most cases the traditional measures might not be sufficient. The decentralized and transparent manner that is one of the blockchain technology applications might hold the answer in ensuring security of IoT systems, as it has been used in device authentication. With the help of an immutable ledger, offered by blockchain, the IoT devices can be registered, authenticated, and verified in a secure way, without involving central authorities, which limits the chances of a cyberattack. The concept of blockchain and IoT combination to offer scalable, secure, and efficient authentication system and its opportunities, disadvantages, and advantages in ensuring the data integrity of interconnected devices is described in the paper.

Keywords: Blockchain, IoT Security, Device Authentication, Decentralization, Scalability

Received Date: 5 June 2025**; Accepted Date:** 15 June 2025**; Published Date:** 20 June 2025.

This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are properly cited.

I. Introduction

The propensity of the farther increase of the connection of IoT devices predicted as 50 billion connections by 2022 significantly grows the chance of an illegal access attempt, hence the necessity to implement an efficient security structure (Pal et al., 2022). A cryptography like blockchain and a distributed consensus-based technology is particularly beneficial to resolve the challenges of security in the IoT ecosystem (Mohammad et al., 2024). Decentralization, immutability, and transparency as the key blockchain properties can make the IoT network create a more constant and steady setting of data
sharing and device administration (Hassan et al., 2019). Blockchain can also be used in a decentralized way to enhance the overall system robustness and availability, removing the single points of failure, which the centralized systems

constitute (Uddin et al., 2021). By entrusting the IoT systems to blockchain, the authors are expecting an extremely secure and faultlessly operating framework, which will become able to eliminate any adverse responses in a chain of societal and environmental factors (Obaidat et al., 2024).

Blockchain and IoT are related and may result in the improvement of security and privacy
but, most of the current research has focused on the high-level abstractions that have not considered the low-level architectural designs

Background of the Study

The Internet of Things paradigm shift has resulted in the geometrical increase in thenumber of connected objects that are changing many various spheres, including healthcare, transport, and smart houses. Nonetheless, such dynamic development has also introduced severe security risks, mainly because the traditional authentication protocols are deficient (regarding managing the scale and the versatility of IoT ecosystems) (Pal et al., 2022). The conventional authentication systems which may rely on the Public Key Infrastructure or a central server are vulnerabilities as they are susceptible to the single point of failure and may be compromised by a myriad of malicious internet activities threatening the whole network (Vangala et al., 2020). The interesting solution to these issues is presented by blockchain technology that has the inherent property of decentralization, immutability, and transparency, and thus, could be used to implement secure and reliable device authentication in a distributed way (Mohammad et al., 2024). Blockchain is decentralized, and that feature allows avoiding the single point of control, reducing the possibility of failure and improving the resilience of the system (Uddin et al., 2021). Through blockchain, Internet of Things devices could mutually authenticate each other without a trusted third party and, in this regard, create a more reliable and secure channel of communication (Obaidat et al., 2024). On top of that, blockchain immutability allows stating that, after a device is authorized and its description is stored on the blockchain, it cannot be changed or faked, which eliminates the possibility of an unauthorized device access and malicious interference (Hassan et al., 2019).

Justification

The general population can employ the Internet of Things devices to enjoy the new connectivity and data-sharing like never before, yet it has become clear that the severe drawbacks of the conventional authentication systems must be overcome (Hassan et al., 2019). The traditional aspect regarding the usage of central authorities in the authentication process of the devices is a single point of failure, and, consequently, the systems of the IoT can be attacked and gain access in a malevolent way (Vangala et al., 2020). One of the new promising technologies showing much potential as the solution to these issues and as the means of ensuring a decentralized and tamper-evident method of securing IoT networks is blockchain (Fernandez-Carames and Fraga- Lamas, 2018; Pal et al., 2022). Another aspect that blockchain substantiates is the reality that only the certificated devices can connect to the IoT networks, which is beneficial to the overall security situation of the systems (Mohammad et al., 2024). Blockchain distributely defines authentication in a node network and thus a central authority point of failure cannot exist, as well as attacks are made resilient (Uddin et al., 2021). Blockchain ledgers are unwritable, and the described property ensures that malicious users could not alter the authentication history to indicate Device identity or access privileges (Pajoohetal. 2021).

Objectives of the Study

1. To explore the possibilities of the blockchain technology to improve the security of the IoT, especially in authentication of the devices.
2. To present the case on the usefulness of decentralized authentication system with regards to fighting threats introduced by IoT networks.
3. To determine the issues and drawbacks of blockchain application in IoT security solution.
4. To suggest an expandable framework of the utilization of blockchain-based authentication system to the IoT devices.
5. To overview the situation in literature and case studies in terms of blockchain and IoT integration and determine whether the

blockchain authentication is effective in comparison to the traditional solutions.

Literature Review

The possibility of an authentication process to devices in networks of the Internet of Things is increasingly being exploited using blockchain technology as an authenticated and decentralized method of authentication (Hassan et al., 2019). Conventional IoT architectures are prone to centralized authentication servers which by their very nature are the points of failure and thus can be compromised. Blockchain provides an attractive and secure alternative that involves spreading the authentication system over a network of nodes, thus making it more resilient and secure (Fernandez-Carames and Fraga- Lamas, 2018). This is due to the fact that the interconnected blockchain through its components where each block contains the record of the transaction can present an imposing line of defense against any data manipulation, and therefore, it would be inconceivably challenging to perpetrate fraud with the records by malicious agents (Mohammad et al., 2024). Blockchain is decentralized, i.e. no one owns the authentication process, and it minimizes the likelihood of manipulation, generating greater trust in inter-device communication in the IoT environment (Pal et al., 2022). In order to make its appeal even more weighty, decentralized character of blockchain will definitely add to the integrity and trust of the IoT networks, as it will decentralize data validation and storage on a vast number of nodes (Vangala et al., 2020). It could be noted that authentication is not the sole use-case of the technology in IoT and it could influence data integrity and accountability by generation of immutable records that ensures transparency and audibility. This aspect of blockchain to remove single points of failure is especially useful in an IoT scenario where the devices connected to each other are numerous and said devices are frequently in hazardous places. This characteristic of decentralization independently adds resistance to Distributed Denial of Service attacks because there is no specific server that can be overwhelmed (Pajooh et al., 2021).

Material and methodology

Based on the literature review and the analysis of the case study, the paper is intended to dwell upon the problem of the blockchain technology applicable to the IoT security systems. It conducts a survey of research papers and industry report and does a prototype implementation of a blockchain-based IoT solution to evaluate the feasibility, benefits, and challenges of using blockchain in device authentication. The paper also discusses the current IoT networks and their vulnerability to a security breach, it compares the efficiency of the traditional authentication systems with the blockchain-based systems. The concept of blockchain-IoT combination is offered and it defines the sequence of activities and elements that are needed to be achieved by the implementation of the scalable and secure authentication of IoT devices.

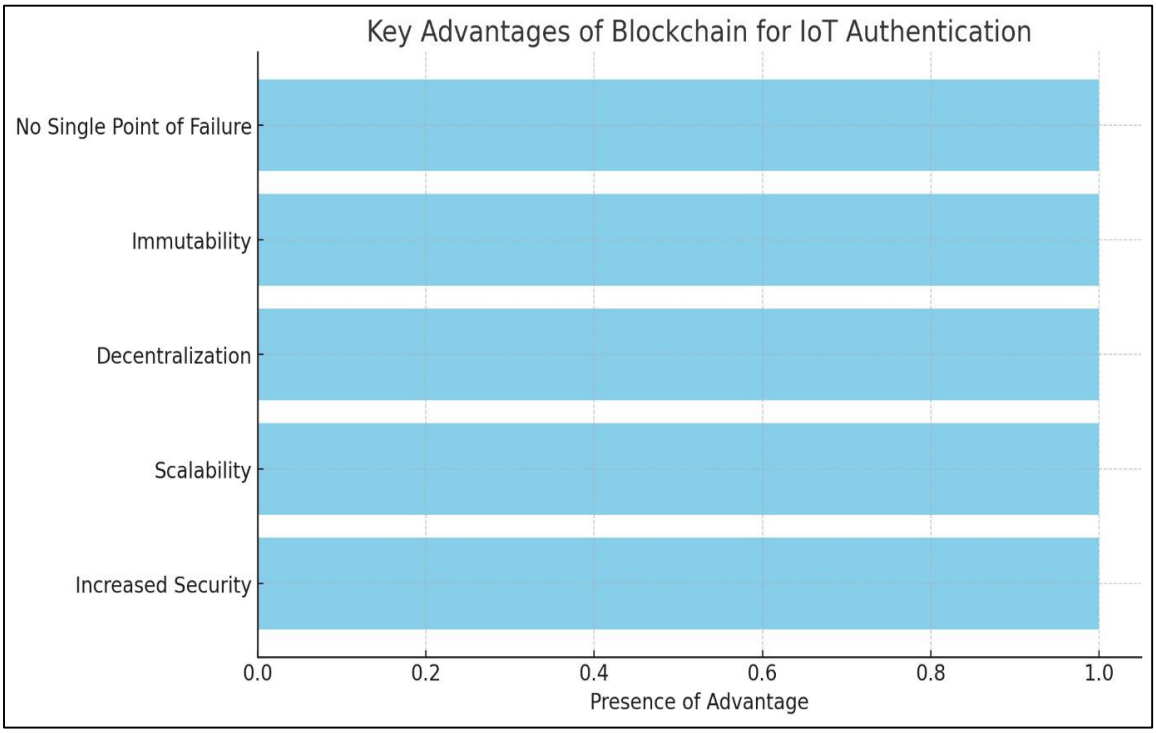
Result and discussion

The advantages of the blockchain and IoT cooperation in authenticating devices are many and contain increased security, scale, and effectiveness. It is this property of blockchain, its decentralization, which allows devices to validate one another without necessarily trusting a central device, removing single points of failure in addition to greatly minimizing the chances of a cyberattack. It is also not possible to alter the credentials of devices without approval due to immutability of blockchain records. Nonetheless, scalability of blockchain to large IoT networks and the energy cost of blockchain transactions are among the obstacles that shall be surmounted. Also, a rather significant obstacle is the interoperability of many IoT devices and blockchain networks. Nevertheless, these issues demonstrate that blockchain has much to work on to make it a reasonable method of improving the security of IoT, but its possible advantages in the field of IoT device authentication are evident.

Table: Blockchain IoT Authentication

Advantages	Description
Increased Security	Blockchain allows devices to authenticate each other without relying on a central authority, ensuring a secure environment.

Scalability	Blockchain enables scalable solutions, making it easier to accommodate an increasing number of IoT devices.
Decentralization	Decentralized nature removes central points of control, reducing risks associated with a single failure.
Immutability	Blockchain ensures that once a device is authenticated, its details cannot be altered, ensuring data integrity.
No Single Point of Failure	Without a single central server, IoT networks are more resilient to attacks such as DDoS.



Some of the prospective advantages of blockchain technology in IoT authentication are improved security, scalability, and decentralization. Blockchain will enable devices to securely authenticate one another, removing the possibility of cyberattacks since it eliminates the necessity of central authorities. Its immutable quality assures information integrity, and because there are no single points of failure, IoT networks become more resilient. All of these features not only make IoT systems more efficient but also offer a more secure and scalable solution to handling such large quantities of interconnected devices.

Study Limitation

Constraints are important to the research since it is based on the secondary data along with other research works. The existing body of knowledge demonstrates the promise of blockchain-based solutions mainly in limited, proof-of-concept scenarios (Singh et al., 2020). The major bottleneck is the lack of larger, real-life deployments that would enable to conduct a highly analytical study of the practical performance and functional ability of blockchain in the complex environment of the IoT security (Chamoli, 2020). Lack of large scale rollouts does not permit the thorough evaluation of

performance levels, resistance to various attack types, as well as the flexibility of blockchain-based IoT security systems to deal with dynamically changing IoT (Uddin et al., 2021). The scalability and energy overheads bottleneck in blockchain is similarly an age-old issue that would require long-term research and development before large-scale applicability of blockchain in authenticating IoT devices can be a reality (Hasan et al., 2024). The blockchain-based technology used in the current system can be faced with the challenge of retaining the interoperability with the legacy technologies and conventional databases that can hinder the smooth integration of the proposed solutions (Hasan et al., 2024).

Future Scope

Among the potential research areas, another line ought to be Hybrid blockchain architectures that cleverly combine the properties of public and private blockchains to overcome the shortcomings of scalability and energy consumption of do-it-yourself blockchain applications (Sadawi et al., 2021). This will entail a close revisit of consensus mechanism, data accessibility management, and governance models in order to configure the most appropriate set up to use in various IoT applications in order to achieve a friendly trade off among transparency, security, and operational efficiency (Khordadpour & Ahmadi, 2024). Standardization of the powerful interoperability solutions is the most important undertaking as it will enable the achievement of interoperability and easycommunication and data exchange among non- homogenous devices in the IoT and heterogeneous blockchain networks (Obaidat et al., 2024). The standardization guidelines, inter- chain communication frameworks, and data translation services can have a significant role in the realization of the functional and nonviolent IoT environment which can help to facilitate the cooperation and breakthrough in many industries (Chamoli, 2020).

Conclusion

The blockchain technology is capable of presenting an efficient, secure and scalable authentication system to the IoT devices that eliminate most of the security challenges that the conventional systems experience. The scalability issues, energy consumption and the lack of interoperability are still there but they do not monopolize the discussion regarding the potential of the blockchain to revolutionize the security of the IoT devices and implementations, this is why it is a promising direction of research and development.

References

1. Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. IEEE Access, 6, 32979. https://doi.org/10.1109/access.2018.2842685
2. Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems, 97, 512. https://doi.org/10.1016/j.future.2019.02.060
3. Mohammad, N., Khatoon, R., Nilima, S. I., Akter, J., Kamruzzaman, Md., & Sozib, H. M. (2024). Ensuring Security and Privacy in the Internet of Things: Challenges and Solutions. Journal of Computer and Communications, 12(8), 257. https://doi.org/10.4236/jcc.2024.128016
4. Pajooh, H. H., Rashid, M. A., Alam, F., & Demidenko, S. (2021). Hyperledger Fabric Blockchain for Securing the Edge Internet of Things. Sensors, 21(2), 359. https://doi.org/10.3390/s21020359
5. Pal, S., Dorri, A., & Jurdak, R. (2022). Blockchain for IoT access control: Recent trends and future research directions. Journal of Network and Computer Applications, 203, 103371. https://doi.org/10.1016/j.jnca.2022.103371
6. Rahman, Z., Yi, X., Mehedi, Sk. T., Islam, M., & Kelarev, A. (2022). Blockchain Applicability for the Internet of Things: Performance and Scalability Challenges and Solutions.

arXiv. https://doi.org/10.48550/arxiv.2205.00384
7. Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2021). A survey on the adoption of blockchain in IoT: challenges and solutions. Blockchain Research and Applications, 2(2),100006. https://doi.org/10.1016/j.bcra.2021.100006
8. Chamoli, S. (2020). Blockchain-based IoT Systems: Techniques, Applications, and Challenges. Türk Bilgisayar ve Matematik Eğitimi Dergisi, 11(3), 2108. https://doi.org/10.17762/turcomat.v11i3.136 08
9. Khordadpour, P., & Ahmadi, S. (2024). Security and Privacy Enhancing in Blockchain-based IoT Environments via Anonym Auditing. arXiv. https://doi.org/10.48550/arxiv.2403.01356
10. Obaidat, M., Rawashdeh, M., Alja'afreh, M., Abouali, M., Thakur, K., & Karime, A. (2024). Exploring IoT and Blockchain: A ComprehensiveSurvey on Security, IntegrationStrategies, Applications and Future Research Directions. https://doi.org/10.20944/preprints202409.1193.v1
11. Sadawi, A. A., Hassan, M. S., & Ndiaye, M. (2021). A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges. IEEE Access, 9, 54478. https://doi.org/10.1109/access.2021.3070555
12. Hasan, H. R., Musamih, A., Salah, K., Jayaraman, R., Omar, M., Arshad, J., & Boscovic, D. (2024). Smart agriculture assurance: IoT and blockchain for trusted sustainable produce. Computers and Electronics in Agriculture, 224, 109184. https://doi.org/10.1016/j.compag.2024.1091 84
13. Prevention. Sensors, 20(14), 3951. https://doi.org/10.3390/s20143951
14. Vangala, A., Das, A. K., Kumar, N., & Alazab, M. (2020). Smart Secure Sensing for
15. Singh, R., Dwivedi, A. D., & Srivastava, G. (2020). Internet of Things Based Blockchain for Temperature Monitoring and Counterfeit Pharmaceutical IoT-Based Agriculture: Blockchain Perspective. IEEE Sensors Journal, 21(16), 17591. https://doi.org/10.1109/jsen.2020.3012294