

International Journal of Engineering Research and Science & Technology



www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2(3) (2026)



ijerst.editor@gmail.com
editor@ijerst.com

Research Paper

Secure Enterprise Networking with Blockchain-Enabled Zero Trust Access Control Systems

Ganta Sairam¹, Kothapalli Prabhas², Shaik Ahammad³, A Varshith⁴, Dr. R. Santhoshkumar⁵

^{1,2,3,4}Students, Department of Computer Science and Engineering, Sree Dattha Group of Institutions, Sheriguda, Ibrahimpatnam, Telangana, India

⁵Associate Professor, Department of Computer Science and Engineering, Sree Dattha Group of Institutions, Sheriguda, Ibrahimpatnam, Telangana, India

Abstract— A robust enterprise networking necessitates stringent protective measures due to the persistent evolution of cyber threats and hazards of unauthorized access. This study aims to enhance company security through the development of a Blockchain-Enabled Zero Trust Access Control System which guarantees secure and reliable user authentication. Conventional enterprise security frameworks depend on perimeter-based defenses, that have become ineffective in dynamic or distributed settings. Certain existing systems implement Zero Trust Architecture and blockchain independently, yielding moderate enhancements in access control and information security. Nonetheless, these methodologies frequently exhibit deficiencies in integration, scalability, and effective real-time authentication procedures. Current research prioritizes individual security techniques over their integration into a cohesive framework. Consequently, the proposed solution amalgamates blockchain technology using Zero Trust concepts to establish a decentralized and immutable access control mechanism. The system comprises secure user registration with login sections, multi-factor authentication, as well as ongoing user verification prior to access authorization. Blockchain is utilized to maintain immutable access logs and oversee identities, guaranteeing transparency and traceability. The integration of these technologies boosts data privacy, improves access regulation precision, and offers superior resistance to

sophisticated cyber attacks, culminating in a more safe and scalable enterprise network solution.

Keywords— Blockchain, Zero Trust Architecture (ZTA), Access Control, Enterprise Security, Multi-Factor Authentication (MFA), Decentralized Identity Management, Cybersecurity, Secure Authentication, Distributed Systems, Data Privacy, Immutable Ledger, Network Security.

I. INTRODUCTION

In recent decades, enterprise networks have experienced substantial transition due to a broad acceptance of cloud computing, remote accessibility, and distributed infrastructures, resulting in enhanced operational flexibility with system complexity [16]. Although these improvements enhance scalability & efficiency, they also increase firms' vulnerability to a rising array of cyber risks, such as data breaches, insider assaults, and unauthorized entry [10]. Conventional security strategies reliant on perimeter defences presume that entities inside the network are trustworthy; however, this presumption is obsolete in contemporary organizational settings where threats may arise from internal as well as external sources [14].

To address these difficulties, Zero Trust Architecture, or ZTA, has arisen as a contemporary security framework founded on the notion of "never trust, always verify," guaranteeing that each access request undergoes rigorous validation [9]. ZTA mandates

ongoing authentication as well as authorization for devices, users, and software irrespective of their location, thus mitigating risks linked to unlawful access & lateral movement within organizational networks [17]. It additionally integrates least-privilege access with real-time monitoring to enhance security enforcement. While ZTA enhances organizational security, its implementation frequently encounters constraints, including centralized control systems, insufficient transparency, and difficulties in preserving safe and tamper-proof access logs [11].

Blockchain technology presents an effective strategy to address these restrictions by delivering a decentralized & immutable framework for the management of identity and access logs [18]. The essential attributes of transparency, data integrity, along with tamper resistance render it exceptionally appropriate for safeguarding corporate systems as well as industrial applications [12]. Integrating blockchain and Zero Trust principles enables the creation of a secure and decentralized access control system which guarantees reliable identification, traceability, and responsibilities across enterprise networks[19].

This article presents a Blockchain-Enabled Zero Trust Access Control System on safe enterprise networking. The suggested methodology integrates decentralized identity management, authentication using multiple factors, & ongoing access verification to eradicate implicit trust and enhance network security. Blockchain is employed to preserve immutable records of authorization and have access actions, guaranteeing transparency and deterring unwanted alterations. The incorporation of these technologies augments data privacy, refines access control precision, and offers robust protection against advancing cyber threats, rendering the system appropriate for contemporary company settings [8].

II. LITERATURE SURVEY

Network automation has swiftly advanced with the incorporation of 5G-supported Industrial Internet of Things (IIoT) systems in Industry 4.0, facilitating effective communication, scalability, with real-time control in industrial settings. As enterprises transition to Industry 5.0, incorporating new technologies like artificial intelligence and human-robot collaboration, the requirements for network automation are increasingly intricate and rigorous. Current methodologies predominantly emphasize existing 5G implementations, although they inadequately address

the forthcoming demands of 6G networks, including ultra-low latency, enhanced dependability, and intelligent automation. This results in a deficiency in comprehending how contemporary technology can be modified or enhanced for future-generation industrial systems. To address this constraint, Hao Ran Chi et al. (2022) [1] conducted an extensive study that evaluates the latest network automation technologies, their standards, and their influence on IIoT inside Industry 4.0. Their research underscores the obstacles and prospective trajectories for network automation as sectors evolve towards 6G-enabled Industry 5.0. The report acts as a significant resource for academics by offering a comprehensive summary of current solutions and a distinct perspective for the advancement of future-generation automated industrial networks.

Industry 4.0 has facilitated industrial advancement over the past decade with the implementation of automation, intelligent systems, and digital technologies; nonetheless, it possesses inherent constraints that hinder its complete potential. Consequently, the notion of Industry 5.0 has arisen, emphasizing cooperation between humans and robots rather than solely depending on automation. This novel methodology seeks to augment efficiency while simultaneously fostering human engagement, creativity, & decision-making in industrial operations. Industry 5.0 prioritizes customized production, enhanced customer happiness, and sustainable development, rendering it essential for contemporary enterprises to maintain competitiveness and attain economic progress. It integrates advanced technologies including the Internet of Things, big data analysis, collaborative robots, blockchain, digital twins, along with emerging communication systems such as 6G to facilitate diverse applications in sectors such as healthcare, manufacturing, supply chain, as well as cloud-based production. The shift to Industry 5.0 presents problems, particularly in managing human-machine interactions and facilitating seamless collaboration in industrial settings. Amr Adel (2022) [5] provide a comprehensive study of these potential, technology, and constraints.

The Industrial Internet of Things (IIoT) is pivotal in converting conventional industrial systems into interlinked & intelligent networks, wherein sensors perpetually assess the state and performance of machinery. This connectivity presents significant issues for security & reliability, as Internet of Things

devices are particularly susceptible to diverse cyber threats, attacks, & malware. Due to the low computing resources of several IIoT devices, they are unable to implement robust built-in security methods, hence heightening the danger of system compromise. Recent strategies have concentrated on employing cloud, fog, as well as edge computing infrastructures to accomplish intricate activities including management of security, data analysis, including decision-making. Khaled Ali Abuhasel et al. (2020)[8] suggested a secure IIoT architecture that improves data protection with an upgraded RSA algorithm and hash-based authentication approaches. Their methodology incorporates an effective clustering technique that considers criteria such as node connection, distance, residual energy, & overall fitness, with optimization realized by the Salp Swarm Algorithm. Additionally, a Soft Max-based deep neural networks is employed for effective resource scheduling to minimize latency & communication overhead. The proposed system exhibits enhanced performance regarding energy efficiency, diminished latency, and fortified security, rendering it appropriate for contemporary industrial applications.

The Industrial Internet of Things (IIoT) features a variety of devices and intricate communication frameworks, complicating data transfer, particularly in wireless settings where security and reliability are crucial issues. Conventional single-path communication techniques frequently lack the capability to guarantee the confidentiality, integrity, & authenticity of critical industrial data, rendering them more susceptible to failures & potential cyberattacks. Mingshi Li et al. (2021) developed secure communication framework with a redundant & collaborative transmission method for smart production line systems to mitigate these restrictions. Their approach utilizes a threshold signature system along with various auxiliary communication channels, ensuring uninterrupted data transmission despite potential failures of some network nodes. This method also mitigates the possibility of data theft by nefarious actors. The system incorporates a predictive approach to restore missing communication data while transmission failures, hence preserving the completeness & consistency of information. Experimental findings indicate that the suggested approach promotes communication accuracy, bolsters data integrity, and strengthens security, rendering it effective for communication

over wireless networks between intelligent devices used in IIoT settings.

SCADA (Supervisory Control and Data Acquisition) systems are extensively utilized in industrial settings and Industrial Internet of Things (IIoT) applications to oversee and regulate essential procedures. Nonetheless, these systems frequently encounter significant security vulnerabilities stemming from inadequate data protection protocols and restricted access control functionalities, rendering them appealing targets for attackers. While encryption mechanisms like SSL/TLS are frequently employed to safeguard data transfer, they may prove inadequate, particularly when data is kept or analyzed on semi-trusted, third-party cloud systems. To address these constraints, Weiting Zhang et al. (2021) suggested a safe and adaptable access control framework that facilitates fine-grained data sharing and includes revocation capabilities. Their methodology improves data confidentiality while offering superior control over access to specific information inside the SCADA system. The strategy additionally integrates digital signature methodologies to guarantee data integrity and avert unlawful alterations. Moreover, it tackles critical obstacles such as insecure communication frameworks, restricted protocol-level security, & trust concerns in cloud environments. Experimental findings indicate that the suggested technology markedly enhances data security with negligible effects on system performance, rendering it a viable alternative for contemporary industrial control systems.

III. DATASET DESCRIPTION

In our proposed study, we utilized a system-generated dataset obtained from the Blockchain-Enabled Zero Trust Access Control System, that tracks real-time user behaviors and data exchanges inside an organizational setting. This dataset comprises many attributes including username, password, contact number, email ID, & address, collected during user registration. The dataset additionally comprises file-related metadata, including file name, owner name, access role (public or private), & blockchain verification hash. Every uploaded file is allocated a distinct hash value, that is recorded by the blockchain to make sure data security and immutability. The dataset additionally records access roles, permitting public files to be accessible by all users while restricting private files to approved users exclusively, hence facilitating secure access management.

The dataset contains user and file data, as well as activity logs that document all user events, including registration, login, file upload, & file download, together with corresponding date and time details. These logs are preserved as blockchain transactions, encompassing details like as block number, transaction hash, & additional metadata to guarantee transparency and traceability. The dynamically created dataset from the system accurately represents real-world enterprise settings where security, authentication, as well as information integrity are paramount. Prior to use the information for evaluation, it may undergo preprocessing activities like record organization, inconsistency removal, and access authorization validation to ensure optimal system performance. This dataset facilitates the analysis of the system's efficacy in maintaining data security, preventing illegal access, and ensuring tamper-proof storage through blockchain technology.

IV. PROPOSED WORK

The deployment of the proposed Blockchain-Enabled Zero Trust Access Control System commences with an intuitive online interface facilitating the registration of new users into the system. During registration, users submit information like username, password, contact number, email address, and physical address. This information is not solely maintained in a conventional database but are also documented as transaction on the blockchain. Every registration produces a distinct transaction with details such as block number & hash value, guaranteeing that the data that has been saved is secure, immutable, and readily verifiable. This stage creates a robust and reliable identity framework for all users within the system.

After a successful registration, users may access the system via the authentication module. The login procedure adheres to Zero Trust principles, wherein each access request is authenticated without supposing any antecedent trust. The system verifies user credentials and authenticates them prior to allowing access. Upon authentication, users are led to the primary dashboard, where they may execute various operations, including data uploads, file access, and activity log reviews. This ongoing verification method aids in thwarting illegal access and enhances overall system security.

The file management module enables users to safely file uploads to the blockchain. In this procedure, users choose a file and designate an access role, including public or private. The system subsequently produces a distinct hash value of the document and

records it on the public blockchain alongside associated metadata. This guarantees that the file remains unaltered without detection, preserving data integrity. Public files are accessible to all users, but private files are limited to the data owners or approved individuals, hence implementing stringent access control into the system.

A key component of the framework is the control of access and data retrieval method. Users can access available files, including information such as file name, owner, & blockchain verification hash. Users are permitted or prohibited from downloading files based on their designated access role. When a user attempts to view personal file with no appropriate authorization, the system restricts access, exemplifying the effective implementation of security protocols. This role-based access safeguards sensitive data while permitting regulated information sharing.

The system contains an activity monitor module that logs all user actions, including registration, login, file uploaded, & file download. Every activity is recorded as a blockchain transactions with timestamps, ensuring the logs are visible and immutable. This facilitates the monitoring of user activities and establishes a definitive audit trail for assessment of security. The amalgamation of blockchain technology with Zero Trust concepts establishes a secure, dependable, and scalable framework for enterprise data management, providing robust safeguards against illegal access and data tampering.

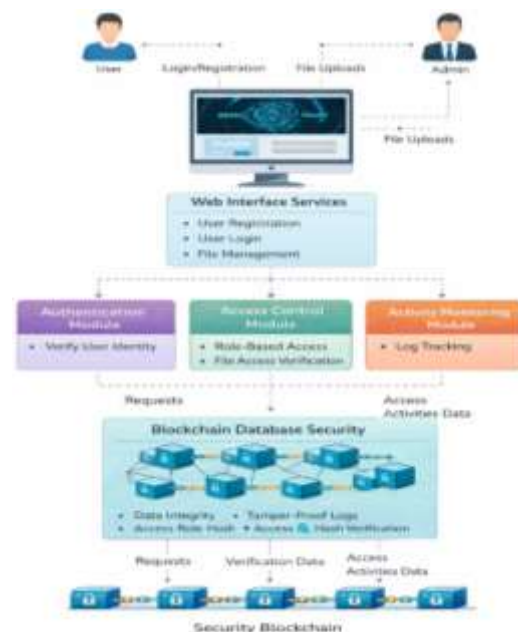


Figure 1: System Architecture for Blockchain-Enabled Zero Trust Access Control System

V. RESULT AND DISCUSSION

The first stage of our suggested solution involves loading the web application user interface. Upon execution of the system, the home screen is presented, serving as the primary interface for user interaction. The interface comprises navigation options including Home, User Login, & New User Signup, directing users to various system functionalities. This screen verifies that the system is now successfully loaded and is prepared for operation. New users may register on this page, while existing users are able to log in to safely access system functionality in accordance with Zero Trust principles. Upon browsing the homepage, new users may register by providing their personal information, including username, password, contact number, email address, and physical address. The registration form collects all essential information needed for identity generation. This measure guarantees that only verified users gain access to the system. The submitted data undergoes validation prior to submission, ensuring data consistency & preventing erroneous inputs.

After finishing the registration procedure, the users may access the system using the login interface. The user must input correct credentials, including a username and password. The system authenticates these details prior to allowing access, adhering to Zero confidence principles that require verification of every access request without presuming prior confidence. This measure guarantees that only permitted users can access the system and utilize its features. Upon successful verification, a user is forwarded to the dashboard for subsequent activities. After a successful registration, users may log in utilizing their credentials. The system authenticates the provided username and password prior to giving access, adhering to Zero Trust principles that require validation of every request. Following successful authentication, the user is led to the dashboard, which offers options including Save Data to Blockchain, Access Data, View Access Activities, & Logout. This dashboard serves as the primary control panel for executing all system functions.

In this phase, users can safely upload files to the blockchain. The system enables users to select a file and designate an access role, like private or public. Upon submission, the system produces a distinct

cryptographic hash for a file and records it on a blockchain system alongside its information. This guarantees the file's integrity, allowing for the swift detection of any alterations. The access role functionality facilitates regulated data dissemination within the system.



Figure 2: File Upload with Access Control Mechanism

The final stage entails retrieving stored data and observing user activities. Figure [2] illustrates that users can obtain file details including the owner's name, file name, blockchain hash, and accessed role. Users are either permitted or prohibited from downloading files based on permissions, hence enforcing Zero Trust access control. The system also preserves a comprehensive activity log that documents all user actions, such as login, upload, & download, accompanied by timestamps. These records are maintained on the blockchain, guaranteeing transparency, traceability, and immutable auditing.



Figure 3: Data Access and Activity Monitoring Interface

DISCUSSION

The development of the proposed Blockchain-Enabled Zero Trust Access Control System demonstrates that enterprise data security may be substantially enhanced by integrating blockchain technology with Zero Trust principles. Existing access control systems frequently depend on centralized storage & implicit trust, rendering them susceptible to unwanted access and data manipulation. The suggested system verifies each user request prior to giving access, thereby reducing

trust assumptions inside the network. The use of blockchain offers an enhanced security layer by preserving user data, file transactions, & activity logs in an unchangeable and tamper-resistant format. The system proficiently oversees authentication of users, secure file uploads, and access control based on roles, ensuring that public as well as private data are managed with suitable limits. The produced hash values for submitted files guarantee data integrity and facilitate straightforward authentication of file authenticity. Additionally, the activity tracking module improves transparency by preserving comprehensive records of all user activities, complete with timestamps. This method enhances security while also ensuring traceability and responsibility within the system. The suggested system exhibits superior reliability, data protection, & resilience against contemporary cyber threats, rendering it appropriate for practical enterprise applications.

VI. CONCLUSION

This aim of project to enhance enterprise network security through the integration of blockchain technology and Zero Trust access control techniques. The suggested solution mitigates the shortcomings of conventional security models by abolishing implicit trust and guaranteeing regular verification of individuals and data access. The system improves data security and inhibits illegal access through the use of decentralised identity management, secured authentication, with role-based access control. Blockchain technology guarantees that all transactions, file information, & activity logs are preserved in an immutable and transparent fashion, hence enhancing confidence and accountability inside the system. The creation of distinct hash values for every file ensures data integrity and facilitates secure data sharing among users. The comprehensive framework exhibits enhanced dependability, security, and scalability relative to current methodologies. This study emphasizes the possibility of integrating blockchain technology with Zero Trust principles to develop resilient enterprise security solutions, hence facilitating secure data management and mitigating risks linked to contemporary cyber threats.

REFERENCES

1. Chi, H. R., Wu, C. K., Huang, N. F., Tsang, K. F., & Radwan, A. (2022). A Survey of Network Automation for Industrial Internet-of-Things Towards Industry 5.0. *IEEE Transactions on Industrial Informatics*.
2. Prassida, G. F., & Asfari, U. (2022). A conceptual model for the acceptance of collaborative robots in industry 5.0. *Procedia Computer Science*, 197, 61-67.
3. Khan, M., Haleem, A., & Javaid, M. (2023). Changes and improvements in Industry 5.0: A strategic approach to overcome the challenges of Industry 4.0. *Green Technologies and Sustainability*, 1(2), 100020.
4. Huang, S., Wang, B., Li, X., Zheng, P., Mourtzis, D., & Wang, L. (2022). Industry 5.0 and Society 5.0—Comparison, complementation and co-evolution. *Journal of manufacturing systems*, 64, 424-428.
5. Adel, A. (2022). Future of industry 5.0 in society: human-centric solutions, challenges and prospective research areas. *Journal of Cloud Computing*, 11(1), 1-15.
6. Carayannis, E. G., Draper, J., & Bhaneja, B. (2021). Towards fusion energy in the Industry 5.0 and Society 5.0 context: Call for a global commission for urgent action on fusion energy. *Journal of the Knowledge Economy*, 12(4), 1891-1904.
7. Abou El Houda, Z., Brik, B., Ksentini, A., Khoukhi, L., & Guizani, M. (2022). When federated learning meets game theory: A cooperative framework to secure iiot applications on edge computing. *IEEE Transactions on Industrial Informatics*, 18(11), 7988-7997.
8. Abuhasel, K. A., & Khan, M. A. (2020). A secure industrial internet of things (IIoT) framework for resource management in smart manufacturing. *IEEE Access*, 8, 117354-117364.
9. Li, Q., Zhang, Q., Huang, H., Zhang, W., Chen, W., & Wang, H. (2022). Secure, efficient, and weighted access control for cloud-assisted industrial IoT. *IEEE Internet of Things Journal*, 9(18), 16917-16927.
10. Mosteiro-Sanchez, A., Barcelo, M., Astorga, J., & Urbieto, A. (2020). Securing IIoT using defence-in-depth: towards an end-to-end secure industry 4.0. *Journal of Manufacturing Systems*, 57, 367-378.

11. Li, M., Yin, Z., Ma, Y., Wang, C., Chai, A., & Lian, M. (2021). Design and verification of secure communication scheme for industrial IoT intelligent production line system with multi-path redundancy and collaboration. *Neural Computing and Applications*, 1-15.
12. Otoum, S., Al Ridhawi, I., & Mouftah, H. (2022). A federated learning and blockchain-enabled sustainable energy-trade at the edge: A framework for industry 4.0. *IEEE Internet of Things Journal*.
13. Jan, Z., Ahamed, F., Mayer, W., Patel, N., Grossmann, G., Stumptner, M., & Kuusk, A. (2022). Artificial Intelligence for Industry 4.0: Systematic Review of Applications, Challenges, and Opportunities. *Expert Systems with Applications*, 119456.
14. Golovianko, M., Terziyan, V., Branytskyi, V., & Malyk, D. (2023). Industry 4.0 vs. Industry 5.0: Co-existence, Transition, or a Hybrid. *Procedia Computer Science*, 217, 102-113.
15. Battini, D., Berti, N., Finco, S., Zennaro, I., & Das, A. (2022). Towards industry 5.0: A multi-objective job rotation model for an inclusive workforce. *International Journal of Production Economics*, 250, 108619.
16. Oztemel, E., & Gursev, S. (2020). Literature review of Industry 4.0 and related technologies. *Journal of intelligent manufacturing*, 31, 127-182.
17. Zhang, W., Zhang, H., Fang, L., Liu, Z., & Ge, C. (2021). A secure revocable fine-grained access control and data sharing scheme for SCADA in IIoT systems. *IEEE Internet of Things Journal*, 9(3), 1976-1984.
18. Li, D., Chen, R., Liu, D., Song, Y., Ren, Y., Guan, Z., ... & Liu, J. (2022). Blockchain-based authentication for IIoT devices with PUF. *Journal of Systems Architecture*, 130, 102638.
19. Xu, Z., Liang, W., Li, K. C., Xu, J., Zomaya, A. Y., & Zhang, J. (2021). A time-sensitive token-based anonymous authentication and dynamic group key agreement scheme for industry 5.0. *IEEE Transactions on Industrial Informatics*, 18(10), 7118-7127.
20. Xu, L., Zhou, X., Tao, Y., Yu, X., Yu, M., & Khan, F. (2021). Af relaying secrecy performance prediction for 6g mobile communication networks in industry 5.0. *IEEE Transactions on Industrial Informatics*, 18(8), 5485-5493.
21. Bhagwat, V. B. (2024). A simplified transition from EBS Payroll to Cloud Payroll: Benefits and Drawbacks. *Journal of Computational Analysis and Applications*, 33(6).
22. Gajula, S. (2024). Cybersecurity risk prediction using graph neural networks. *Journal of Information Systems Engineering and Management*, 9(4), 3301-3315. <https://doi.org/10.52783/JISEM.V9I4S.13885>
23. Venkata Ramana, P. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. *International Journal of Research in Information Technology and Computing*, 8(4).
24. Shashank, A. (2025). AI-Enhanced ETL Processes: Leveraging Artificial Intelligence for Optimized Data Integration Systems. *Journal Of Multidisciplinary*, 5(8), 219-225.
25. Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.
26. Maturi, S. Y. (2021). Blockbond hardening: Securing pooled-hash protocols against traffic tampering, MITM hash-rate hijacking, and template coercion. *International Journal of Communication Networks and Information Security*, 13(3), 718-728.
27. Maturi, S. Y. (2023). Crowdsourced frontier: Unveiling autonomous adversarial cybercapabilities via open AI competition. *International Journal of Intelligent Systems and Applications in Engineering*, 11(1s), 275-284.
28. Kumar Adabala, P. (2021). Optimizing ERP Modernization: A Smart Data Migration Framework Approach. *International Journal of Enhanced Research in Science, Technology & Engineering*, 10(07), 61-72. <https://doi.org/10.55948/ijerste.2021.0708>
29. Gummadi, V. P. K. (2023). MuleSoft batch processing: High-volume streaming

- architecture. *Computer Fraud & Security*, 50-57. <https://doi.org/10.52710/cfs.886>
30. Shashank, A. (2025). Self-Healing Data Pipelines for Enhanced Reliability: A Paradigm Shift in Enterprise Data Management. *Journal of Computer Science and Technology Studies*, 7(8), 1097-1104.
31. Ghali Krishna Harshitha. A Study on the Impact of Ethical Attitude of Managers on Organizational Climate. *World Journal of Management and Economics*, pp. 1–5.
32. Boyapati, P. K., Susarla, R. S., & Kandula, S. T. R. (2025, April). Revolutionizing Fraud Detection in Real-Time Financial Transactions Using AI-Based Boundary-Integrated Neural Networks with Starfish Optimization Algorithm. In *International Conference on Computer Vision and Robotics* (pp. 75-87). Cham: Springer Nature Switzerland.
33. Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. *IJSAT-Int. J. Sci. Technol.* 16 (2).
<https://doi.org/10.71097/IJSAT.v16.i2.3219>