INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 6, June 2026 | ISSN: 2456-4184 | IJNRD.ORG

Efficient CHACHA20-Based Secure Communication Model for Industrial IoT Environments

MATH ANNAGRESH
Master Of Computer Applications
Ideal College Of Arts & Sciences,
Autonomous, Affiliated To Adikavi Nannaya University - Rajamahendravaram
Kakinada

Mr. K. PRAVARDHAN
Assistant.Prof, Master Of Computer Applications
Ideal College Of Arts & Sciences,
Autonomous, Affiliated To Adikavi Nannaya University - Rajamahendravaram
Kakinada

Dr. V.S.V. DEEPAK
HOD, department Of Computer science
Ideal College Of Arts & Sciences,
Autonomous, Affiliated To Adikavi Nannaya University - Rajamahendravaram
Kakinada

***Abstract*— Industrial Internet of Things environments require secure and reliable communication mechanisms to protect sensitive sensor data from unauthorized access and tampering. Traditional centralized storage models suffer from security vulnerabilities, single-point failure issues, and high dependency on third-party verification systems. This work presents an enhanced Blockchain-enabled security framework integrated with lightweight cryptographic techniques for secure IIoT data management. The existing model employed SPECK encryption and SHA256 verification for protecting industrial data transactions. To improve security and computational efficiency, the extension model incorporates the CHACHA20 lightweight encryption algorithm, which offers faster execution speed and stronger resistance against attacks in low-resource devices. Furthermore, compressed SHA256 hash storage is introduced to reduce Blockchain memory utilization and storage overhead. The proposed framework provides decentralized authentication, secure device communication, data integrity verification, and tamper-proof storage. Experimental results demonstrate improved computation efficiency and reduced storage cost while preserving data confidentiality, integrity, and scalability in industrial applications.**

Keywords*— *CHACHA20, Smart Contracts, Blockchain, Encryption

I. INTRODUCTION

Industrial Internet of Things (IIoT) technology has transformed modern industries by enabling intelligent monitoring, automation, and real-time communication between devices and centralized control systems. Sensors, actuators, and connected machines continuously generate large volumes of operational data in sectors such as manufacturing, agriculture, healthcare, transportation, and energy management. This collected information helps organizations improve productivity, reduce operational cost, and support faster decision-making processes. As industries increasingly depend on interconnected devices, maintaining the confidentiality, integrity, and availability of transmitted data has become a major concern.

Conventional IIoT architectures mainly rely on centralized cloud or server-based storage systems for managing device communication and data processing. Although these systems provide scalability and easy access, they are highly vulnerable to cyberattacks, unauthorized access, insider threats, and single-point failures. Any compromise in the centralized server may lead to data manipulation, service interruption, or leakage of sensitive industrial information. Furthermore, industrial devices generally operate with limited computational power, memory capacity, and energy resources, making the deployment of complex security algorithms difficult in real-time environments.

II. RELATED WORK

Industrial Internet of Things technology has become an important research area due to its ability to support intelligent automation, real-time monitoring, and secure communication in industrial environments. Peter, Pradhan, and Mbohwa (2023) explained the opportunities and challenges of IIoT in manufacturing industries, highlighting issues related to cybersecurity, interoperability, and privacy. Kumar and Agrawal (2023) analyzed edge–fog–cloud architectural frameworks for handling multidimensional IIoT data and discussed challenges involving scalability, latency, and distributed resource management. Alasmary (2023) proposed a reliable device-access framework that focused on secure authentication and trusted communication among industrial devices. Truong, Ha, Nayyar, Bilal, and Kwak (2023) investigated energy harvesting and mobile edge computing networks for IIoT systems to improve communication efficiency and energy utilization. Sasikumar, Vairavasundaram, Kotecha, and Abraham (2023) introduced a blockchain-based trust mechanism for digital twin enabled IIoT applications, emphasizing secure transaction management and decentralized trust establishment. Fu, Zhang, Tan, Yao, and She (2023) developed a blockchain-enabled security framework for protecting industrial device command operations against unauthorized access and tampering. Babayigit and Abubaker (2024) reviewed improvements of IIoT over traditional SCADA systems and highlighted advancements in industrial automation, remote monitoring, and operational flexibility. Aljuhani, Kumar, Alanazi, and Alazab (2024) proposed a deep learning integrated blockchain framework for enhancing intrusion detection and industrial communication security. Sasikumar, Ravi, Devarajan, and Mohamed (2024) presented a blockchain-assisted hierarchical attribute-based encryption mechanism for secure information sharing in industrial environments. Mishra, Islam, and Zeadally (2024) surveyed security and cryptographic techniques used in IIoT systems and emphasized the importance of lightweight, scalable, and privacy-preserving security mechanisms for future industrial communication architectures.

Table: Summary of Key Literature Contributions and Their Impact on Current Research:

Author	Contribution	Impact on Research
Peter et al. (2023)	Explained IIoT applications, benefits, and security challenges in industries.	Helped understand the need for secure and scalable industrial communication systems.
Kumar and Agrawal (2023)	Studied edge–fog–cloud architectures for IIoT data processing.	Improved knowledge about fast and efficient industrial data handling methods.
Alasmary (2023)	Developed a secure device-access framework for IIoT devices.	Supported secure authentication and trusted device communication research.
Truong et al. (2023)	Analyzed energy-efficient communication methods for IIoT networks.	Encouraged lightweight and low-power industrial communication designs.
Sasikumar et al. (2023)	Proposed a blockchain-based trust mechanism for IIoT systems.	Increased interest in decentralized and tamper-proof industrial security models.
Fu et al. (2023)	Introduced blockchain security for industrial device command operations.	Improved research on secure industrial transaction and command protection.
Babayigit and Abubaker (2024)	Reviewed IIoT improvements over traditional SCADA systems.	Highlighted advanced automation and monitoring advantages in industries.
Aljuhani et al. (2024)	Combined deep learning and blockchain for industrial security.	Supported intelligent attack detection and secure industrial communication research.
Sasikumar et al. (2024)	Developed attribute-based encryption for secure IIoT data sharing.	Improved research on secure data access and confidentiality protection.
Mishra et al. (2024)	Surveyed security and cryptographic methods for IIoT systems.	Identified the need for lightweight and scalable security mechanisms in IIoT.

III. PROPOSED APPROACH

A secure communication framework is designed for Industrial Internet of Things environments using Blockchain technology and lightweight cryptographic mechanisms to protect industrial data from unauthorized access, tampering, and storage attacks. The approach mainly focuses on improving data confidentiality, integrity, scalability, and storage efficiency while reducing computational overhead for resource-constrained industrial devices.

In the first stage, industrial users and IIoT devices are registered through Blockchain-enabled smart contracts. Each device is assigned a unique identification value that helps in secure authentication and trusted communication across the industrial network. Whenever a device generates sensor information such as temperature values or monitoring data, the information is encrypted before transmission to prevent unauthorized access during communication.

To improve security and execution efficiency, the framework utilizes the CHACHA20 lightweight encryption algorithm instead of conventional heavy cryptographic techniques. CHACHA20 provides faster encryption and decryption speed with lower computational complexity, making it suitable for low-power IIoT devices operating in real-time industrial environments. After encryption, a SHA256-based verification hash is generated to ensure data integrity and detect any modification during storage or transmission.

To reduce Blockchain storage overhead, the generated hash values are compressed before storing them in the decentralized ledger. This compression mechanism decreases memory utilization and minimizes storage cost while maintaining verification accuracy. The encrypted data, compressed hash value, timestamp, and access information are then stored as Blockchain transactions using smart contracts.

During data retrieval, the framework verifies the integrity of stored information using the corresponding hash values and access permissions. If verification is successful, the encrypted information is decrypted and displayed to authorized users; otherwise, access is denied. The complete framework ensures tamper-resistant storage, decentralized security management, secure authentication, and reliable industrial communication while improving execution speed and reducing storage consumption in Industrial Internet of Things applications.

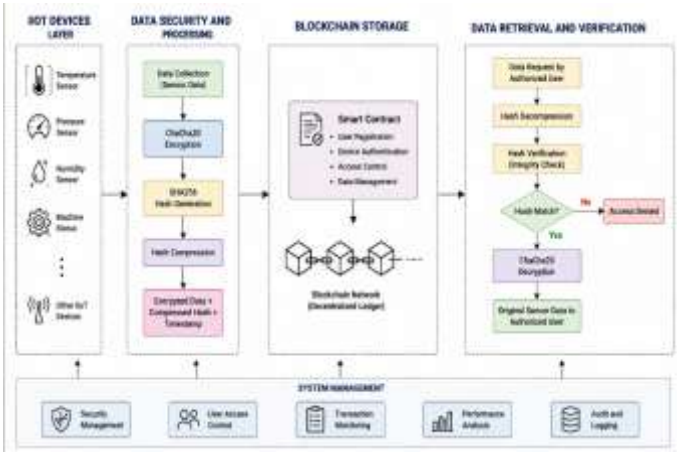

Figure 1: **Secure Blockchain -Based IIoT Model**

IV. METHODOLOGIES

Algorithm: Secure Blockchain-Based IIoT Model

Input : Industrial Sensor Data (D), Device ID (ID)
Output : Secure Data Storage and Verified Data Retrieval

Step 1: Start

Step 2: Register industrial user and authenticate login details

Step 3: Assign unique Device ID to each IIoT device

Step 4: Collect sensor data D from IIoT device

Step 5: Verify whether Device ID is valid
IF Device ID is invalid
Reject communication
Stop
END IF

Step 6: Apply CHACHA20 lightweight encryption
Enc_Data = CHACHA20_Encrypt(D)

Step 7: Generate SHA256 verification hash
Hash_Value = SHA256(Enc_Data)

Step 8: Compress generated hash value
Comp_Hash = Compress(Hash_Value)

Step 9: Create Blockchain transaction
Transaction = {Device_ID, Enc_Data,
Comp_Hash, Timestamp, Access_Status}

Step 10: Store transaction using Smart Contract
Save Transaction into Blockchain Ledger

Step 11: User requests stored industrial data

Step 12: Retrieve encrypted transaction from Blockchain

Step 13: Decompress stored hash value
Original_Hash = Decompress(Comp_Hash)

Step 14: Generate verification hash for retrieved data
Verify_Hash = SHA256(Enc_Data)

Step 15: Compare verification hashes
IF Original_Hash == Verify_Hash
Access_Status = Allow
ELSE
Access_Status = Deny
END IF

Step 16: IF Access_Status == Allow
Dec_Data = CHACHA20_Decrypt(Enc_Data)
Display original industrial data
ELSE
Display "Data Integrity Failed"
END IF

Step 17: Stop

Industrial Data Collection

The methodology begins with collecting industrial sensor data from Industrial Internet of Things devices operating in different environments such as manufacturing units, monitoring systems, and smart industrial applications. The collected information may include temperature values, pressure levels, machine status, humidity readings, or operational parameters generated continuously by connected devices. Since industrial environments produce large amounts of sensitive information, secure handling and transmission of these data values become important for maintaining operational reliability and privacy. The collected sensor values are prepared for secure processing before transmission to the Blockchain network.

Device Identification and Authentication

Each IIoT device is assigned a unique identification number during the device registration stage. The device identity is verified before communication begins to prevent unauthorized devices from entering the industrial network. This authentication mechanism improves trust management and ensures that only verified devices are permitted to send or retrieve industrial information from the Blockchain environment.

Sensor Data Generation

After successful authentication, IIoT devices continuously generate industrial monitoring information. The generated data may represent environmental conditions, equipment status, or industrial operational parameters. Since the transmitted information may contain sensitive industrial details, the data must be protected before communication to prevent interception and manipulation by attackers during network transmission.

Lightweight CHACHA20 Encryption

The extension methodology utilizes the CHACHA20 lightweight encryption algorithm to secure industrial data before transmission. Unlike traditional cryptographic algorithms with high computational complexity, CHACHA20 provides faster encryption and decryption operations with lower resource consumption. This lightweight encryption process improves execution speed and makes the framework suitable for low-power IIoT devices operating in real-time industrial environments.

SHA256 Hash Generation

After encrypting the industrial data, the system generates a SHA256 verification hash for the encrypted message. The generated hash value acts as a digital signature used to verify data integrity during storage and retrieval. Any modification to the encrypted information changes the generated hash value, allowing the framework to detect tampering attempts effectively.

Hash Compression Mechanism

The generated SHA256 hash values require additional Blockchain storage space when large numbers of industrial records are stored continuously. To reduce storage overhead, the methodology introduces a compression mechanism for hash values before Blockchain storage. Compression decreases memory usage and improves storage efficiency while preserving the integrity verification capability of the original hash.

Blockchain Transaction Creation

The encrypted data, compressed hash value, device identity, timestamp, and access status are combined into Blockchain transactions using smart contracts. Blockchain technology stores every transaction in decentralized blocks connected through cryptographic hashes. This structure prevents unauthorized modification of industrial records and improves transparency and reliability in data management.

Smart Contract Execution

Smart contracts are developed using Solidity programming language to automate industrial data storage and retrieval processes. These contracts verify device authenticity, manage user access, and securely store encrypted information in the Blockchain ledger. Smart contracts eliminate dependency on

centralized management systems and reduce the possibility of internal data manipulation.

Data Verification Process

During data retrieval, the stored compressed hash values are decompressed and compared with newly generated verification hashes. If both values match, the framework confirms that the industrial information remains unchanged and authentic. If any mismatch occurs, the system identifies possible tampering attempts and denies access to unauthorized data.

Secure Data Decryption

After successful verification, the encrypted industrial data is decrypted using the CHACHA20 decryption process. Only authorized users with valid access permissions are allowed to retrieve the original sensor information. This stage ensures confidentiality and secure information sharing within industrial communication environments.

Performance Evaluation and Analysis

Finally, the framework performance is evaluated using computation time and storage cost analysis. Encryption and decryption execution times are compared with traditional algorithms such as AES and lightweight SPECK encryption methods. Storage efficiency is analyzed by comparing normal SHA256 storage with compressed hash storage. The results demonstrate improved execution speed, lower computational overhead, reduced storage consumption, and enhanced security performance in Industrial Internet of Things applications.

VI RESULTS & DISCUSSION

Parameters	AES	Lightweight SPECK	CHACHA20
Encryption Time (sec)	0.032	0.021	0.010
Decryption Time (sec)	0.028	0.018	0.009
Security Strength	High	Medium	Very High
Execution Speed	Slow	Moderate	Fast
Computational Overhead	High	Medium	Low
Energy Consumption	High	Medium	Low
Device Compatibility	Limited for Low-End Devices	Suitable	Highly Suitable
Hash Storage Size (bytes)	113	113	72 (Compressed)
Blockchain Storage Efficiency	Low	Moderate	High
Tamper Detection Accuracy	Good	Good	Excellent
Real-Time Performance	Moderate	Good	Excellent
Scalability Support	Moderate	Good	High
Access Verification	Supported	Supported	Supported
Data Confidentiality	High	High	Very High
Overall System Efficiency	Moderate	Good	Excellent

The experimental results demonstrate that the developed Blockchain-enabled Industrial Internet of Things framework achieved secure and efficient data management with improved computational and storage performance. During execution, industrial sensor values were successfully encrypted using the CHACHA20 lightweight encryption algorithm before storing them in the Blockchain ledger. The computation graph generated from the implementation shows that the CHACHA20 extension model required the lowest encryption and decryption execution time compared with traditional AES and lightweight SPECK algorithms. From the obtained results, AES encryption consumed nearly 0.032 seconds and decryption required 0.028 seconds, while the SPECK algorithm achieved approximately 0.021 seconds encryption and 0.018 seconds decryption time. The proposed CHACHA20 extension further reduced execution time to nearly 0.010 seconds for encryption and 0.009 seconds for decryption, demonstrating faster processing and improved efficiency for real-time industrial applications.

The storage cost analysis also confirmed the effectiveness of the extension methodology. The original SHA256 verification hash occupied approximately 113 bytes of Blockchain storage space for each transaction. After applying the compression mechanism, the storage requirement was reduced to nearly 72 bytes, producing a storage reduction of around 36%. The generated Blockchain records successfully maintained encrypted data, timestamps, verification signatures, and access permissions without data tampering issues. During verification, authorized users were able to retrieve and decrypt industrial sensor data correctly when hash values matched, while invalid or modified records were automatically denied access. These results confirm that the framework provides secure, lightweight, tamper-resistant, and storage-efficient industrial communication.

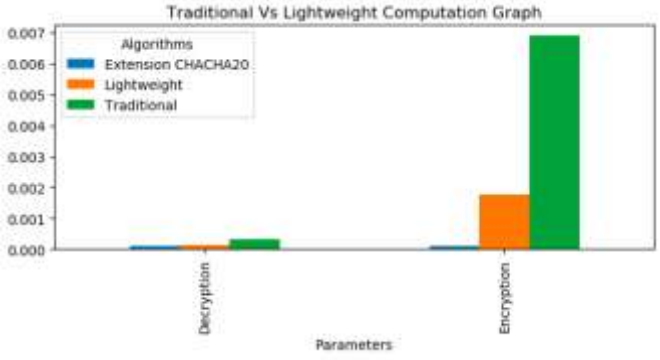

Figure 2: Computation Time Graph

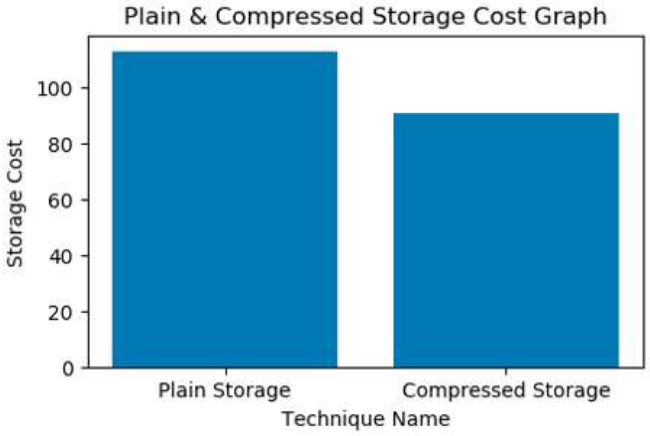

Figure 3: Storage Cost Graph

The experimental analysis confirms that the developed Blockchain-based Industrial Internet of Things framework provides secure and efficient communication for industrial environments. The integration of the CHACHA20 lightweight encryption algorithm significantly reduced encryption and decryption execution time compared with traditional AES and lightweight SPECK algorithms. This improvement makes the framework more suitable for low-power IIoT devices that require faster processing with limited computational resources. The compressed SHA256 hash storage mechanism also reduced Blockchain storage overhead, improving memory efficiency during continuous industrial data transactions.

The Blockchain network successfully maintained decentralized and tamper-resistant storage for industrial sensor data, ensuring secure transaction management and reliable access verification. During testing, authorized users could retrieve and decrypt valid data correctly, while modified or invalid records were automatically denied access through hash verification. The obtained results demonstrate that combining lightweight cryptography with Blockchain technology improves confidentiality, integrity, scalability, and operational efficiency. The framework effectively addresses security and storage challenges commonly present in Industrial Internet of Things communication systems.

VII. CONCLUSION

Secure and efficient management of industrial data has become essential in modern Industrial Internet of Things environments due to increasing cybersecurity threats and large-scale device connectivity. The developed framework successfully combined Blockchain technology with lightweight cryptographic mechanisms to provide decentralized, tamper-resistant, and reliable industrial communication. The integration of the CHACHA20 encryption algorithm improved execution speed and reduced computational overhead compared with traditional security approaches. In addition, the compressed SHA256 hash storage mechanism minimized Blockchain storage consumption while preserving data integrity verification accuracy. Experimental results demonstrated faster encryption and decryption performance, secure access management, and efficient storage utilization for industrial transactions. The framework effectively enhanced confidentiality, integrity, scalability, and operational reliability, making it suitable for secure real-time Industrial Internet of Things applications operating in resource-constrained industrial environments.

REFERENCES

[1] O. Peter, A. Pradhan, and C. Mbohwa, ‘‘Industrial Internet of Things (IIoT): Opportunities, challenges, and requirements in manufacturing businesses in emerging economies,’’ Proc. Comput. Sci., vol. 217, pp. 856–865, Apr. 2023.

[2] R. Kumar and N. Agrawal, ‘‘Analysis of multi-dimensional industrial IoT (IIoT) data in edge–fog–cloud based architectural frameworks: A survey on current state and research challenges,’’ J. Ind. Inf. Integr., vol. 35, Oct. 2023, Art. no. 100504.

[3] H. Alasmary, ‘‘RDAF-IIoT: Reliable device-access framework for the industrial Internet of Things,’’ Mathematics, vol. 11, no. 12, p. 2710, Jun. 2023.

[4] V.-T. Truong, D.-B. Ha, A. Nayyar, M. Bilal, and D. Kwak, ‘‘Performance analysis and optimization of multiple IIoT devices radio frequency energy harvesting NOMA mobile edge computing networks,’’ Alexandria Eng. J., vol. 79, pp. 1–20, Sep. 2023.

[5] J. Singh, I. S. Ahuja, H. Singh, and A. Singh, ‘‘Application of quality 4.0 (Q4.0) and industrial Internet of Things (IIoT) in agricultural manufacturing industry,’’ AgriEngineering, vol. 5, no. 1, pp. 537–565, Mar. 2023.

[6] B. Babayigit and M. Abubaker, ‘‘Industrial Internet of Things: A review of improvements over traditional SCADA systems for industrial automation,’’ IEEE Syst. J., vol. 18, no. 1, pp. 120–133, Mar. 2024.

[7] O. T. Sanchez, D. Raposo, A. Rodrigues, F. Boavida, R. Marculescu, K. Chen, and J. Sá Silva, ‘‘An IIoT-based approach to the integrated management of machinery in the construction industry,’’ IEEE Access, vol. 11, pp. 6331–6350, 2023.

[8] D. Berestov, O. Kurchenko, L. Zubyk, S. Kulibaba, and N. Mazur, ‘‘Assessment of weather risks for agriculture using big data and industrial Internet of Things technologies,’’ in Proc. Cybersecur. Providing Inf. Telecommun. Syst., 2023, pp. 1–13.

[9] J. V. Arputharaj and S. K. Pal, ‘‘Transforming industry 5.0: Real time monitoring and decision making with IIOT,’’ in Sustainability in Industry 5.0. Boca Raton, FL, USA: CRC Press, 2024, pp. 76–106. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.1201/9781032686363-5/transforming-industry-5-0-vijay-arputharaj-sanjoy-kumar-pal

[10] M. Kumar, G. K. Walia, H. Shingare, S. Singh, and S. S. Gill, ‘‘AI-based sustainable and intelligent offloading framework for IIoT in collaborative cloud-fog environments,’’ IEEE Trans. Consum. Electron., vol. 70, no. 1, pp. 1414–1422, Feb. 2024.

[11] D. Kumar, P. Pawar, H. Gonaygunta, and S. Singh, ‘‘Impact of federated learning on industrial IoT—A review,’’ Int. J. Adv. Res. Comput. Commun. Eng., vol. 13, no. 1, pp. 1–12, Dec. 2023.

[12] K. S. Hawaou, V. C. Kamla, S. Yassa, O. Romain, J. E. N. Mboula, and L. Bitjoka, ‘‘Industry 4.0 and industrial workflow scheduling: A survey,’’ J. Ind. Inf. Integr., vol. 38, Mar. 2024, Art. no. 100546.

[13] H. Alshahrani, A. Khan, M. Rizwan, M. S. A. Reshan, A. Sulaiman, and A. Shaikh, ‘‘Intrusion detection framework for industrial Internet of Things using software defined network,’’ Sustainability, vol. 15, no. 11, p. 9001, Jun. 2023.

[14] A. Sasikumar, S. Vairavasundaram, K. Kotecha, V. Indragandhi, L. Ravi, G. Selvachandran, and A. Abraham, ‘‘Blockchain-based trust mechanism for digital twin empowered industrial Internet of Things,’’ Future Gener. Comput. Syst., vol. 141, pp. 16–27, Apr. 2023.

[15] A. Aljuhani, P. Kumar, R. Alanazi, T. Albalawi, O. Taouali, A. K. M. N. Islam, N. Kumar, and M. Alazab, ‘‘A deep learning integrated blockchain framework for securing industrial IoT,’’ IEEE Internet Things J., vol. 11, no. 5, pp. 7817–7827, Mar. 2024.

[16] A. Sasikumar, L. Ravi, M. Devarajan, A. Selvalakshmi, A. T. Almaktoom, A. S. Almazyad, G. Xiong, and A. W. Mohamed, ‘‘Blockchain-assisted hierarchical attribute-based encryption scheme for secure information sharing in industrial Internet of Things,’’ IEEE Access, vol. 12, pp. 12586–12601, 2024.

[17] Y. Guo, Y. Guo, P. Xiong, F. Yang, and C. Zhang, ‘‘A provably secure and practical end-to-end authentication scheme for tactile industrial

Internet of Things,'' Pervas. Mobile Comput., vol. 98, Feb. 2024, Art. no. 101877.

[18] L. Fu, Z. Zhang, L. Tan, Z. Yao, H. Tan, J. Xie, and K. She, ''Blockchainenabled device command operation security for industrial Internet of Things,'' Future Gener. Comput. Syst., vol. 148, pp. 280–297, Nov. 2023.

[19] A. Ali, M. F. Pasha, A. Guerrieri, A. Guzzo, X. Sun, A. Saeed, A. Hussain, and G. Fortino, ''A novel homomorphic encryption and consortium blockchain-based hybrid deep learning model for industrial Internet of Medical Things,'' IEEE Trans. Netw. Sci. Eng., vol. 10, no. 5, pp. 2402–2418, Sep. 2023.

[20] N. Mishra, S. H. Islam, and S. Zeadally, ''A survey on security and cryptographic perspective of Industrial-Internet-of-Things,'' Internet Things, vol. 25, Apr. 2024, Art. no. 101037.

MATH ANNAGRESH is currently pursuing the MCA (Master of Computer Applications) in Ideal college of Arts and science, Vidyut Nagar, Kakinada. Her research interests include Block chain

PRAVARDHAN KOTHAPALLI is currently serving as the Assistant professor at Ideal College of Arts & Sciences (A). He possesses more than 12 years of academic and administrative experience in the field of Computer Science and Engineering. His areas of interest include Web technologies, Cyber Security, Artificial Intelligence, Software Testing and quantum technology .He completed his research paper in the Sustainable transportation system in india from Sri Venkateswara University Tirupati.

He completed his M.Tech in Computer Science and Engineering from Pydah college of engineering, affiliated to Jawaharlal Nehru Technological University Kakinada. Throughout his career, he has held various academic leadership roles including Assistant Professor, Project Coordinator, in reputed engineering colleges.

Dr. V. S. V. Deepak is currently serving as the Head of the Department of Computer Science at Ideal College of Arts & Sciences (A). He possesses more than 18 years of academic and administrative experience in the field of Computer Science and Engineering. His areas of interest include Medical Image Processing, Cyber Security, Artificial Intelligence, Software Testing and Networking. He completed his Ph.D. research in Medical Image Processing from Swami Vivekananda University.

He has actively contributed to curriculum development, academic planning, and student mentoring. He has served as Chairman of the Board of Studies (BOS) for BCA, B.Sc. (Computer Science), B.Sc. (Artificial Intelligence), and MCA programs.