ETDT

Emerging Trends in Digital Transformation

Volume-2, Issue-1, January-March 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-20***

BLOCKCHAIN-BASED CYBER THREAT DETECTION FOR IOT NETWORKS USING DEEP LEARNING

[#1]G. LAKSHMI, ***Associate Professor,***
[#2]SAFURA MAHEROZE, ***B.Tech Student,***
[#3]VEDUMALAPELLI SRINIJA, ***B.Tech Student,***
[#4]BODDUPALLI SRINIVAS, ***B.Tech Student,***
[#5]CHILUVERU KUMAR, ***B.Tech Student,***
Department of AIML,
TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TG.

ABSTRACT: The Industrial Internet of Things (IIoT) is a powerful Internet of Things (IoT) application that revolutionizes industry development by promoting open communication across various organizations, including centers, manufacturing facilities, and packaging facilities. The current IIoT systems are devoid of data science methodologies, which the IIoT can leverage to more effectively analyze acquired data, as a result of their distributed structure. The IIoT is at a substantial security risk due to network assaults and anomalies. In order to prevent fraudulent devices from joining the network, this investigation employs a coordinator IoT device to ascertain the trustworthiness of IoT devices. Furthermore, the implementation of a blockchain-based data paradigm promotes data transparency. The efficacy of the proposed system is meticulously and exhaustively verified against a diverse array of security metrics, including the likelihood of false authentication, the strength of an attack, and the likelihood of message tampering, using MATLAB. The simulation results indicate that the proposed method enhances the security of IIoT networks by effectively identifying hostile network threats.

Keywords—*Industrial Internet-of-Things (IIoT), Blockchain, Security, Secure IoT Devices, Trust Management*

1. INTRODUCTION

The performance and profitability of a company are currently contingent upon its methods of accumulating and analyzing financial data. There will be more and more chances for this technology to advance as data science and related businesses grow. More than 6 billion devices can connect to the internet as of 2016. They produce 2.5 quintillion bytes of data per day as a collective.

Effective real-time data analysis equipment were lacking. The IoT and other smart gadgets and sensors that meet client needs allow these products to communicate. Data science uses rigorous scientific methods, algorithms, procedures, and systems to find significant patterns and insights in vast databases. Data science in the IoT (DS-IoT) improves data collection, processing, and accuracy. Transportation, cyber-physical systems, and healthcare workers use sensors to generate production data and keep records. The DS-IoT improves system interoperability.

DOI: https://doi.org/10.5281/zenodo.19017728

Volume-2, Issue-1, January-March 2026 ISSN: 3107- 4308 Paper ID: ETDT-V2-I1-20

The ability of devices to produce their own data is essential for the Internet of Things, and the DS-IoT paradigm has been praised for this. time efficiency. Examples of Internet of Things (IoT) applications that aim to improve decision-making by managing various physical assets necessary for scaling trials include smart cities, e-healthcare, intelligent transportation, and Industrial Internet of Things (IIoT).

An important use case for the Internet of Things (IoT) is the Industrial Internet of Things (IIoT), which keeps tabs on and reports on everything happening in the industrial sector to help it expand. A network of interconnected computing devices that can exchange data with one another is known as the Internet of Things (IoT).

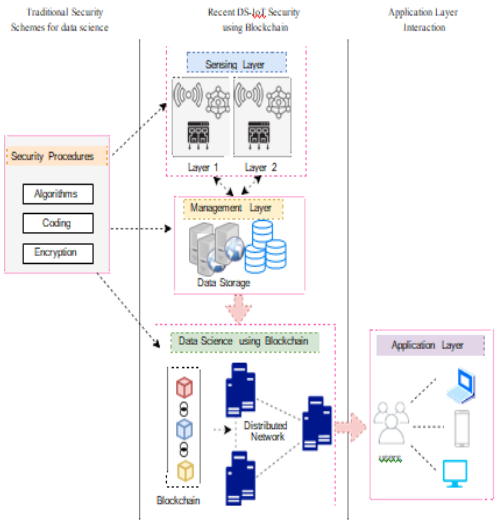

Fig. 1: DS-IoT Blockchain in Industrial IoT

Businesses are hesitant to implement IoT devices because of security concerns, even though DS-IoT technology has several benefits. By interfering with communication data or blocking reliable IoT devices from sending accurate data, an errant IoT device might reduce network performance within typical industry standards. Some open-source ciphers still have security holes, but they're being fixed all the time by many people, so bad changes made by centralized or outside parties don't matter.

All smart gadgets are supposed to work together and be consistent in most businesses. Unfortunately, IoT devices can be compromised by malicious devices (MD). Differentiating between mediocre and excellent DS-IoT devices may be crucial to enabling open discourse. Keep the public's trust and guarantee data security by notifying data owners of changes to their information as soon as possible . To prevent future data manipulation in smart devices, there have been recent ideas to use blockchain technology. A sequence of blocks comprised of data collected by Internet of Things devices throughout a product's manufacture and distribution are archived by a blockchain network, as shown in Figure 1.

The efficient and transparent analysis and manipulation of data is made possible by blockchain technology. Every time someone makes a change to the data, a blockchain will keep track of it. The IIoT makes it possible for automated devices to communicate with one another, which means they can handle several events at once.

Quick action and covert monitoring are made possible in this way. To make sure IIoTs can handle data well, process it, and gather it, the data science plan is in place. Despite DS-IoT's

DOI: https://doi.org/10.5281/zenodo.19017728

Volume-2, Issue-1, January-March 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-20***

widespread use in industry, many businesses and organizations are still wary about adopting it. Internet of Things alternatives are more difficult to implement due to the high expense of server infrastructure and centralised cloud computing. No indication that IIoT employs DS-IoT security via blockchain was identified by the author in the cited articles.

Internet of Things (IoT) devices provide extremely private data in an industrial Internet of things (IIoT) setting, including boiler temperature, product production history, and shipment details. Building security into the IIoT network's design from the beginning should be its top priority. If bad nodes in the IIoT network can change data from IoT devices, the network could be attacked. This has me thinking about how to build a network that can both protect data from assaults and make it easy for devices to share data with each other.

2. PROPOSED INDUSTRIAL BLOCKCHAIN FRAMEWORK

The efficacy of our methodology was demonstrated by evaluating it on an IIoT network that included both benign and malicious nodes. There is a system model that backs up the suggested structure. When it comes to DS-IIoT, the security of data analysis is guaranteed by integrating blockchain technology into the IIoT network. To measure how well the network is doing, a mathematical model is created. To solve problems like decentralized information distribution, internal access control, and privacy concerns when several parties exchange data, CU can use blockchain technology to build control and data-sharing platforms. As shown in Figure 2, a system that is built on the blockchain allows anybody to access and trace the history of all documents created by a particular company. Intentional creation or alteration of a data record would be quickly exposed by blockchain technology.

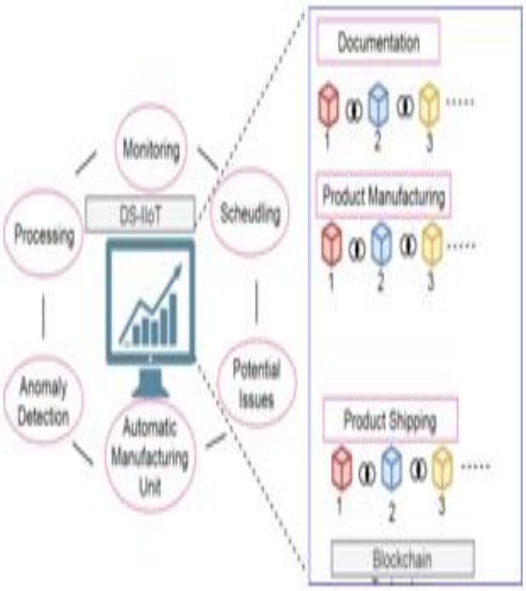

Fig. 2: Data Model of DS-IIoT using Blockchain

DOI: https://doi.org/10.5281/zenodo.19017728

Volume-2, Issue-1, January-March 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-20***

Algorithm 1: Execution of Proposed IIoT Framework

Assumption: $Count_{threshold}$ = 50%
Input: (1) Network with 'n' IDs, (2) Among them one CID is elected, and (3) 'm' number of MD's
Output: ID identified as either legitimate or malicious
The CID selection is based on ST, energy level and MC.
CID maintains a table having ID id, ID address, routing information, CID id, ST and TF of each ID to identify MD. Upon the emergence, the NID is identified as MD else legitimate.
if *(ID is NID)* **then**
    CID allows first five assumptions and;
    Compute TF();
    Compute MC();
    Blockchain record ();
    The information of each record corresponding to ID is stored in the database with its current and previous hashes.
else
    ID is elected as MD
end

3. RELATED WORK

Data science and blockchain technology research has led to the discovery of ways to protect IIoT networks. In order to investigate problems with processing industrial big data, Yan et al. offered a multi-source dataset that was specifically structured for different situations. This approach works well with many datasets owned by the same company. In order to conduct data-driven business operations, the authors examined smart devices' data storage, processing, and application capabilities. They didn't think about data security or the possibility of illegal access.

Stream and bulk data processing, distributed access and storage, real-time control—all of these are capabilities of the state-of-the-art industrial data processing system that Wang and colleagues have created. According to , traditional data processing technologies are insufficient for the massive amounts of data needed for the Industrial Internet of Things (IIoT). Storage, connection via intermediary nodes, and expensive transmission are just a few of the potential challenges that may arise from compiling such a massive data set. For this reason, researchers aren't stopping until they find a way to guarantee the safe transfer of data via trustworthy intermediaries.

Blockchain is now the most effective method for many IIoT organizations to increase the security, privacy, trust, and decentralization of their operations. S. Yu et al. developed a blockchain-based data transmission technique with high economic transfer value and low transaction costs.

The purpose of this implementation was to guarantee the safety of data transfer between Internet of Things devices. Smart device mapping, the consent algorithm, and distributed

DOI: https://doi.org/10.5281/zenodo.19017728

network architecture are some of the methodologies used to assess smart devices' decentralized autonomy. Concerns about the security and privacy of Internet of Things devices were discussed in a paper by Y. Yu et al. Distributed ledger technology (blockchain) enabled Internet of Things (IoT) architecture has many benefits, such as guaranteed scalability, decentralized procedures, and payment-related data transmission authentication. Additional evidence for the phenomenon may be found in concrete Ethereum solutions that showcase the integration of blockchain technology with the Internet of Things. The feasibility of hacking Internet of Things devices using either public or private blockchain was not addressed in the research.

An approach to secure data exchange in the IoT industry is provided by Oh et al. The authors found the best way to maximize profits for everyone by using the Nash equilibrium to determine the viability of the market. In order to facilitate data transmission and storage among Internet of Things devices, Hasan et al. created an interplanetary file system. Smart contracts, algorithms, system implementation approaches, and schematics have all been thoroughly tested for security in the authors' blockchain-based solution.

The authors have proven that their alternative approach is superior to the present one. The importance of the problem prompted Lam et al. to create an autonomous, decentralized system for orchestration and configuration. During the planning and production stages, the suggested technology was used to transmit data over the cloud within an IIoT framework. The results of this use were then reviewed.

Despite several suggestions for keeping IIoT networks decentralized, open, and secure, there has been less investigation into the various techniques used by hackers to interrupt operations or exhaust network resources. Data storage, processing, and nodes in blockchain-based IIoT networks were not validated using trust-based approaches, either, by the writers.

The data science techniques that could revolutionize the internet of things have been the subject of a great deal of research. There has been little focus on blockchain security as it pertains to industrial IoT. By combining data science with blockchain technology, the IIoT network can make industrial data analysis more efficient and dependable. By combining data science with blockchain to detect network vulnerabilities, this research gives the Industrial Internet of Things (IIoT) a solid and modern basis. Our planned organizational structure will be discussed in further detail in the section that follows.

4. RESULTS

The effects on the real network devices caused by a hacked Internet of Things device are shown in Figure 4. The absence of a trust-based structure makes IoT devices an attractive target for hackers. In its present form, the system uses a trust-based structure for member authentication, which blocks phony devices from joining the system. Because of this, there is less of a chance that an Internet of Things device will be hacked and do damage.

The proposed phenomenon has more benefits since CID can distinguish TF according to their actions. Figure 7, like Figure 6, shows that the anticipated phenomena is amplified when compromised miners are included. Because the selection of miners is based on their Trust

Factor (TF), attackers are unable to easily swap out miners while configuring the network. Down below, we detail some more limitations on this publishing.

The usefulness of the blockchain-based solution for data exchange in IIoT networks cannot be adequately proved by comparing security measures with existing approaches alone. This is because the blockchain is a decentralized protocol. To the best of our knowledge, no one has developed data science strategies for the Industrial Internet of Things (IIoT) that make use of blockchain technology. In the second place, the network can be more susceptible to security issues due to the fact that the block verification mechanism makes validation more difficult. The proposed system would be rendered incapable of making intelligent decisions while the transmission of real-time data is taking place as a result of this.

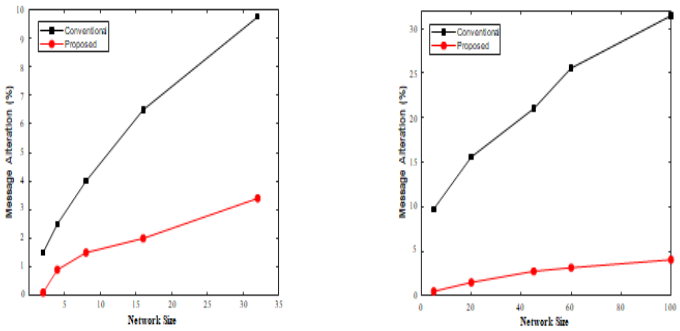

Fig. 3: Message Alteration for (a) Small Network (b) Large Network

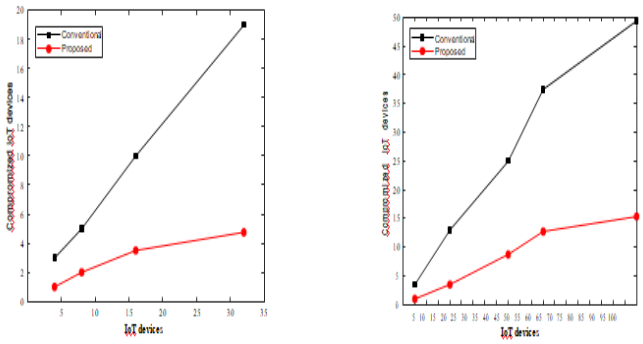

Fig. 4 Compromised IoT deivces for (a) Small Network (b) Large Network

5. CONCLUSION

The trust-based architecture and secure blockchain developed in this research tackle the many problems caused by rogue devices in IIoT networks. By utilizing a designated Coordinator IoT Device (CID), the suggested paradigm determines an IoT device's permissibility by calculating its Trust Factor (TF). To keep an eye on what's happening in the factory and stop anyone from tampering with the local database, they use a data architecture based on the blockchain. There has been extensive testing of the method using a range of network sizes and evaluation metrics. Simulation results show that our proposed method outperforms the network without a blockchain by 91%.

DOI: https://doi.org/10.5281/zenodo.19017728

REFERENCES

[1] A. Karpatne, G. Atluri, J. H. Faghmous, M. Steinbach, A. Banerjee, A. Ganguly, S. Shekhar, N. Samatova, and V. Kumar, "Theory-guided data science: A new paradigm for scientific discovery from data," IEEE Transactions on Knowledge and Data Engineering, vol. 29, no. 10, pp. 2318–2331, 2017. doi:10.1109/TKDE.2017.2720168.

[2] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things Based Smart Cities: Recent Advances and Challenges," IEEE Communications Magazine, vol. 55, no. 9, pp. 16–24, 2017. doi: 10.1109/MCOM.2017.1600514.

[3] H. Oh, S. Park, G. M. Lee, H. Heo, and J. K. Choi, "Personal data trading scheme for data brokers in iot data marketplaces," IEEE Access, vol. 7, pp. 40120–40132, 2019. doi:10.1109/ACCESS.2019.2904248.

[4] P. A. Merolla, J. V. Arthur, R. Alvarez-Icaza, A. S. Cassidy, J. Sawada, F. Akopyan, B. L. Jackson, N. Imam, C. Guo, Y. Nakamura, et al., "A million spiking-neuron integrated circuit with a scalable communication network and interface," Science, vol. 345, no. 6197, pp. 668–673, 2014. doi:10.1126/science.1254642.

[5] C.-X. Wang, F. Haider, X. Gao, X.-H. You, Y. Yang, D. Yuan, H. M. Aggoune, H. Haas, S. Fletcher, and E. Hepsaydir, "Cellular architec- ture and key technologies for 5g wireless communication networks," IEEE communications magazine, vol. 52, no. 2, pp. 122–130, 2014. doi:10.1109/MCOM.2014.6736752.

[6] E. Bertino and N. Islam, "Botnets and internet of things security," Computer, no. 2, pp. 76–79, 2017. doi:10.1109/MC.2017.62.

[7] L. Zhou, D. Wu, J. Chen, and Z. Dong, "When computation hugs intelligence: Content-aware data processing for industrial iot," IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1657–1666, 2017. doi:10.1109/JIOT.2017.2785624.

[8] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial iot: Blockchain system with credit-based consensus mechanism," IEEE Transactions on Industrial Informatics, 2019. doi:10.1109/TII.2019.2903342.

[9] F. Al-Turjman and S. Alturjman, "Context-sensitive access in indus- trial internet of things (iiot) healthcare applications," IEEE Transac- tions on Industrial Informatics, vol. 14, no. 6, pp. 2736–2744, 2018. doi:10.1109/TII.2018.2808190.

[10] J. Wan, J. Li, M. Imran, and D. Li, "A blockchain-based solution for enhancing security and privacy in smart factory," IEEE Transac- tions on Industrial Informatics, vol. 15, pp. 3652–3660, June 2019. doi:10.1109/TII.2019.2894573.

[11] J. A. Shamsi and M. A. Khojaye, "Understanding privacy violations in big data systems," IT Professional, vol. 20, no. 3, pp. 73–81, 2018. doi:10.1109/MITP.2018.032501750.

[12] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, and D. Chen, "Enhancing cloud-based iot security through trustworthy cloud service: An integra- tion of security and reputation approach," IEEE Access, vol. 7, pp. 9368– 9383, 2019. doi:10.1109/ACCESS.2018.2890432.

[13] H. Moosavi and F. M. Bui, "Delay-aware optimization of physical layer security in multi-hop wireless body area networks," IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 1928–1939, 2016. doi:10.1109/TIFS.2016.2566446.