Journal of Applied Engineering and Technological Science
Vol 7(1) 2025: 631-646

BLOCKCHAIN FRAMEWORK FOR SECURE IOT OPERATIONS IN MILITARY APPLICATIONS: INTEGRATING LORAWAN AND HELIUM NETWORK

Jebarani Evangeline S[1*], Krishna Prakash Arunachalam[2], Seethalakshmi V[3], Senthil Kumar A[4], Reeda Lenus C[5], Saranya R[6]
Associate Professor, Department of Electrical and Electronics Engineering, SNS College of Engineering, Coimbatore, Tamilnadu, India[1]
Departamento de Ciencias de la Construcción, Facultad de Ciencias de la Construcción Ordenamiento Territorial, Universidad Tecnológica Metropolitana, Santiago, Chile[2]
Associate Professor, Department of Artificial Intelligence and Data Science, R.M.K. College of Engineering and Technology, Thiruvallur, Tamilnadu, India[3]
Professor, Department of Computer Science and Engineering, School of Engineering, Dayananda Sagar University, Bangalore, India[4]
Department of Physics, S.A. Engineering College, Chennai, Tamilnadu, India[5]
Assistant Professor, Department of Electrical and Electronics Engineering, Velammal College of Engineering and Technology, Madurai, Tamilnadu, India[6]
reachjebarani@gmail.com

Received: 16 October 2024, Revised: 19 August 2025, Accepted: 25 August 2025
**Corresponding Author*

ABSTRACT
The traditional IoT is typically based on centralized systems that are susceptible to multiple cyberattacks and a single point of failure. Modern industries regularly embrace block chain technology due to its decentralization and security. This study suggests a block chain-based system that guarantees reliable and secure operations. They suggest a secure compact block chain for handling access to precious information through instruments and controllers. Based on realistic military applications, the current investigation makes evidence for the benefits of merging LoRaWAN and Helium Network technology, and also demonstrates how deliberate research and analysis can bridge the block chain gap for military cyber defense. To improve the proposed system's computing efficiency, the block chain network has devised a rapid and power-saving decision technique for proof of authentication. The suggested framework for smart industrial environments has survived extensive testing and study to be sustainable. Use the suggested configuration to convert a standard processing system into an intelligent and secure industrial platform. This article aims towards assessing the practicality of Proof of Authority in the block chains network as a consensus algorithm. There are numerous techniques available for creating a consensus among the nodes.
Keywords: *Block chain, Internet of Things (IoTs), services, Military application, LoRaWAN, Helium Network, cyber security, Proof of Authority Algorithm.*

1. Introduction

For both industry and academia, new business and research opportunities have emerged thanks to block chain and Internet of Things (IoT) technology. The distributed environment serves as the foundation for the basic characteristics of block chain, and participant sharing of ledgers between organizations is a reasonable response to a number of IoT-related problems. The topologies of block chain and IoT are comparable (Viriyasitavat et al., 2019). Numerous offerings provided via IoT platforms, such as big data analysis, edge and remote computing, high-speed social networking, and mobile app development, can be valuable to modern industries (Latif et al., 2021; Suhail et al., 2021).

Ahmad et al. (2021), have proposed, an exciting new technology called blockchain holds great promise for the aerospace and defense sectors in a number of ways, including decentralized trust, data security and integrity, traceability, transparency, visibility, and auditability. Bockchain platforms will be evaluated for their suitability and applicability to aerospace and defense applications. Aseri et al. (2024), have discussed One revolutionary invention that has changed how society interacts and communicates is the blockchain. It might be described as a chain of

blocks that saves data with digital markers in a decentralized network. Blockchain technology, which has not yet been evaluated for military applications, has the potential to shift some digital frameworks' security flaws from a weak link weakness model, where an attacker only needs to consider the hub to ignore the framework. Ayan et al. (2022), With a focus on its growing use in sectors including food, agriculture, and healthcare, this study suggested how blockchain technology promotes sustainability in supply chains. Traceability, Industry 4.0, and disruptions brought on by pandemics are important themes. Bhawna et al. (2023), have proposed a bibliometric analysis is to present qualitative and quantitative information on the constantly changing topic of blockchain application in consumer services in an orderly fashion. It is combined with a systematic literature review (SLR) using the SPAR-4-SLR protocol with the theories, characteristics, contexts, and methods framework. Azbeg et al. (2022) have proposed the as a cutting-edge solution to address the security issues in IoT-based systems, blockchain is of great interest. Motivated by these concerns, this paper presents BlockMedCare, a safe healthcare system that combines IoT and Blockchain.

Yazdinejad et al. (2020), This paper proposes applying a blockchain-based authentication methodology to improve drone security and reduce latency in smart city scenarios. Using a zone-based design and a proprietary consensus method known as Drone-based Delegated Proof of Stake (DDPOS), the system avoids the need for frequent reauthentication. The findings of the experiment demonstrate enhanced security and performance, effectively detecting 97.5% of aerial drone threats. Zakaret et al. (2022), This study describes a hybrid security method for energy smart meter gateways that combines blockchain and Secure Element (SE) technology to assure data immutability and secure data production. The SE provides a trustworthy computing foundation, establishing a solid foundation of trust in IoT contexts. This solution has been tested across many implementations and provides safe, decentralized peer-to-peer energy trade using LPWAN and blockchain.

Akter et al. (2022), have suggested to integrating blockchain technology for safe data access with CNN for precise illegal UAV localization through RF signal analysis, the IoMT-Net improves military UAV security. In IoMT situations, its excellent DoA estimation accuracy guarantees trustworthy threat detection. Galán et al. (2022) have suggested, the military environment produces a lot of data that is very important, thus analyzing it requires the application of machine learning. Mohril et al. (2021), have suggested the variety of equipment and deployment sites, maintaining military equipment is difficult but essential for battle readiness. This paper describes a blockchain-based architecture for securely managing detailed maintenance data. The design uses smart contracts to automate monitoring and validation. It ensures little human interaction and meets military-specific maintenance requirements. Sokolović et al. (2023), have recommended the Internet of Things makes it possible to monitor the energy and supply chain, coordinate manufacturing, optimize equipment performance, transport, promote public health, and enhance worker safety and health. IoT services will undoubtedly contribute to increased automation and improved quality of military decisions on the battlefield, particularly in the face of unexpected scenarios in an unpredictable hostile environment, allowing for a reduction in both human and material losses during operations. Wrona et al. (2019), This study investigates how blockchain technology might improve security in military settings, particularly in situations like civil-military cooperation when building a shared trust basis is challenging. It suggests storing metadata from crowdsourced sensors and the Internet of Things on blockchain, guaranteeing safe and reliable information exchange. The high-level architecture is presented in accordance with STANAG 4774 and 4778, two NATO specifications. The report also includes a technical implementation with Hyperledger Fabric and identifies outstanding problems. Zhu et al. (2020), have described, a blockchain technology's revolutionary potential in military operations, particularly when combined with big data, cloud computing, IoT, and AI. It is anticipated that its future applications would improve military command, security, administration, and support systems. Exploring and anticipating blockchain's influence is crucial for increasing combat effectiveness and fostering military innovation.

In this area, block chain technology, which is still in its infancy, has advanced in resolving difficult market issues pertaining to data security and product lifecycle management. By using block chain, businesses may fix key traceability defects, control data on a shared distributed ledger

is not under one person's control and is shared by all participating entities, and securely, immutably, and permanently record events (Viriyasitavat et al. 2019, Yadav et al. 2024, Rathee et al. 2019). Immutability, auditability, and disintermediation are features of block chain that guarantee the execution of processes and the integrity of data in interoperation (De Villiers, et al. 2021). Device deployment can be problematic for IoT devices since they have their distinctive requirements, which include radio coverage, scalability, and power consumption.

The upcoming advancement in general area, low power wireless communications has been designated Low Power broad Area Network, or LPWAN. Similar to currently available long-range IoT wireless communications technologies, LoRaWAN, an open specification subset of LPWAN and Long Range, functions inside around the world unlicensed frequency bands, removing licensing costs while keeping this technology affordable and globally deployable (Singh, et al. 2020, Khan et al. 2022). Following this, at least a few governments have promoted distinct block chain schemes at the level of safeguarding the internet. Tenneti et al. (2024), This study investigates the potential hazards to military communications posed by jamming assaults on blockchain-enabled Helium network devices. It presents the Wolfpack algorithm, which determines the best quantity and location of jammers to disrupt network operations. In such decentralized systems, the results demonstrate the resilience provided by hotspot redundancy as well as the danger posed by sophisticated jamming techniques. Rammouz et al. (2023), The security flaws in blockchain enabled Helium devices which offer decentralized, inexpensive wireless Internet for Internet of Things systems are examined in this paper. Researchers examined darknet traffic from roughly 1 million devices spread throughout the globe to identify hazards affecting 6,000 Helium hotspots. The findings identified around 869,000 suspicious occurrences and vulnerabilities in 62,000 locations. The findings reveal substantial dangers to the confidentiality, integrity, and availability of Helium networks. Reyneke et al. (2023) have reported, financial incentives offered by the Helium Network bitcoin blockchain have been utilized to encourage gateway owners to set up a backup network from their residences and places of business, accelerating the adoption and deployment of LoRaWAN in both urban and rural locations. Along with being simple to set up, the Helium Network offers improved security by using a public blockchain ledger to confirm the sender and recipient's identities in order to thwart man-in-the-middle and packet replay attacks. Mtetwa et al. (2022), In order to secure firmware transmission via a low data rate, restricted LoRaWAN, this study attempts to create a security architecture that uses Blockchain and the InterPlanentary File System (IPFS). The suggested security paradigm protects integrity, secrecy, availability, and authentication while focusing on resource-constrained low-power devices. A proof of concept was put into place and assessed using low-powered devices to show the usefulness and applicability of the suggested paradigm. Rammouz et al. (2023), This article examines possible security risks of blockchain-enabled Helium Internet of Things devices, which offer inexpensive, decentralized wireless connectivity. By examining 2.9 TB of unwanted Internet traffic, the team discovered over 860K darknet events associated to thousands of Helium hotspots. Additionally, it exposes 62K devices to medium-to-critical vulnerabilities, underscoring serious security issues in this expanding network. Krueger et al. (2024), have proposed to determine whether LoRaWAN telemetry might be used for high-altitude balloons, a series of test flights were undertaken over Wyoming, which had very few public LoRaWAN Gate gateways. The public LoRaWAN network received and transmitted to our servers over 95% of the flight telemetry, which surprised us. Hope et al. (2024), have proposed A secure authentication mechanism for LoRaWAN nodes that binds them to on-chain NFTs for proof-of-authenticity and improves LoRaWAN security. The plan works with the current LoRaWAN requirements, which include additional computed information and the microcontroller ID as part of the uplink message payload along with sensor data in this case, temperature. Applications can be grouped into different groups related to their intended use, such as data integrity, swarming drones, a decentralized military network, a trustworthy supply chain for arms, and members' authorization (Yu, et al. 2018, Huo, et al., 2022). In recent years, there has been an interesting an increase in the use of private block chains by multiple companies for a range of use cases, such finance, supply chain management, and data verification for automobile. Since Ethereum is a well-performing public block chain with an effective capability for smart contracts that can be deployed for private networks, we focus on it. Particularly, Ethereum has

grown in popularity (Wu, et al., 2022) and is being evaluated for private chains by multiple companies that have security, user verification, privacy, and rapidly transaction processing issues.

In private chains, Proof of Authority (PoA) consensus dominates over Proof of Work (PoW) consensus because to reap the advantages of demonstrated attendees, predictable consensus, performance, and efficiency (Suhail, et al., 2022). we explore the theoretical performance limits for Ethereum-based block chains to discover bottlenecks and the reasons behind them in each client. We report the challenge that result from multiple forks in the the Clique algorithm, fork deadlock, and Geth being a node stagnating at the EVM layer to the Go-Ethereum community (Wang, et al. 2022, Viriyasitavat, et al., 2019). which are being monitored and fixed. Although the former is a more structured implementation, we indicate the challenges and primary contributors here for the other clients, Parity and Besu.

All over the world, the explosion of digital information is rising at a rapid rate due to the emergence of social media and the internet. At the same time copyrighted content protection has been recognized as an imperative necessity. When launching their work, makers of content need to be comfortable that they can stop piracy. Violent upon copyright produces monetary harm for creators, builders, and politicians. It discourages creative thought and impedes technological and entrepreneurial advancement (Ceccarelli, et al., 2020).

International treaties on copyright protection operate instead of the notion of international copyright laws. The term "national treatment" refers to the notion that in the event that a copyright infringement occurs in a foreign country and the convention is in effect, the copyright owner is considered as a citizen of that country and is obliged to comply with its national copyright laws (Honar Pajooh, et al. 2021, Bataineh et al., 2022). The Bern Convention fails to establish a special court for conducting national treatments; instead, the treatments are practiced in the towns and cities of the foreign nations where the copyright infringements occurred.

The Helium Network is a decentralized wireless infrastructure based on LoRaWAN technology. LoRaWAN offers long-range, low-power communication, making it suitable for IoT devices that need to operate over large geographic areas while using minimal energy. The Helium Network uses blockchain technology to enable individuals and businesses to construct hotspots that provide network coverage while receiving cryptocurrency rewards. This concept eliminates the need for centralized telecom providers while providing a scalable, cost-effective, and secure solution for connecting IoT devices in industrial, urban, and distant settings. This proposed study focuses on solving the security and reliability issues in traditional, centralized IoT systems. The main goal is to create a decentralized blockchain-based system that ensures secure access to sensitive data, especially in industrial and military settings. It also explores the use of LoRaWAN and Helium Network for strong, long-range communication and tests Proof of Authority as a faster, more energy-efficient consensus method. The aim is to build a smart, secure, and sustainable industrial platform. In IoT and blockchain-based systems, data integrity ensures that information communicated and stored is correct and unaffected, preventing tampering or corruption. Authentication checks the identification of devices and users which access the system, ensuring that only authorized entities can interact with sensitive data or resources. Network resilience refers to a system's ability to continue operating reliably despite failures, attacks, or disturbances, which is especially important in decentralized and mission-critical situations such as military or industrial networks.

Contribution of this Work

The following are the contribution of the proposed approach, for further information:

- Proposes a compact blockchain framework to enhance security and reliability in IoT systems, particularly for sensitive information access through instruments and controllers.
- Demonstrates the effectiveness of combining LoRaWAN and Helium Network technologies for secure, long-range communication in military applications.
- Introduces a power-efficient and rapid decision-making method based on Proof of Authority to improve computing efficiency in the blockchain network.

- Validates the system's sustainability and adaptability through extensive testing, proving its feasibility in transforming conventional systems into smart, secure industrial platforms.

2. Literature Review

Xie et al. (2019), Dhar et al. (2021) This study investigates the combination of blockchain and Software-Defined Networking (SDN) in Vehicle Ad-hoc Networks (VANETs) with specific reference to the need for secure communication in the Internet of Things (IoT). The authors speak about the encouraging advancement of trust in distributed electronic systems, through the use of blockchain, particularly in a 5G ecosystem. The suggested structure resolves the problem of security weaknesses existing in older-model systems.

Latif et al. (2021), The article by Latif et al. proposes an architecture of the Internet of Things aimed at the protection of the industrial Internet of Things. The authors also claim that the main reason for the risks posed by data and information breaches is the need for strict adherence to a centralized system. The architecture uses smart contracts for secure transactions thus facilitating efficient operations and reliability of the system.

Li et al. (2021), This paper presents a critical evaluation of research on trust management systems based on blockchain technology, which operates within a cloud computing environment. The authors explain the details of different models and protocols for trust enhancement with the use of popular technologies and their potential in IoT device and service management. The review provides recommendations for further studies focusing on the area of improving system interoperability and scalability.

Sharma et al. (2023), The authors explore the implications of cyber security and blockchain technologies in the 'battlefield of things.' This demonstrates the usefulness of blockchain as a safe communication tools and data sharing information systems for military IoT devices where problems such as unauthorized access and data integrity must be solved. The authors accentuate the concern of safeguarding classified military information against unauthorized parties.

Pióro et al. (2024), Here, the recipient is fully aware where the information is limited to. Such mechanisms help overcome the problem of protecting data from unauthorized users since ABE can be folly implemented. The paper shows how addressing security issues under this framework could work in military aspect of the system.

Reyneke et al. (2023), Pavithran et al (2020) This paper looks into the feasibility study for applications of LoRaWan and Helium blockchain technology in military and other IoT ecosystems. Believe FC meets the many levels advantages of these communications technologies in military operations. The paper gives practical examples of use cases and also presents challenges and prospects of deploying blockchain into military IoT systems.

Although various studies have examined security in blockchain-based IoT systems, specific challenges remain unresolved, particularly in terms of energy efficiency, scalability, and suitability for mission-critical contexts such as military operations. Many previous solutions still rely on computationally intensive consensus techniques, rendering them unsuitable for low-power IoT devices. Furthermore, safe and reliable long-distance communication is frequently disregarded because most frameworks do not incorporate technologies such as LoRaWAN and the Helium Network. Furthermore, there is a scarcity of focused research on how blockchain might be modified to fulfill the real-time and robust security requirements of smart industrial and military systems, leaving a void in practical, implementable solutions.

Previous research has investigated blockchain in IoT to improve security and decentralization, but it frequently relies on energy-intensive consensus methods such as Proof of Work, which are unsuitable for low-power or real-time industrial applications. Furthermore, little study has been conducted on employing blockchain in military settings or merging it with long-range communication technologies like as LoRaWAN and the Helium Network. This study fills such gaps by presenting a compact, energy-efficient blockchain system based on Proof of Authority, specifically built for secure and smart industrial and military applications.

Research Gap

While traditional IoT systems often rely on centralized architectures that are vulnerable to cyberattacks and single points of failure, much of the existing research in blockchain-IoT integration still lacks a tailored approach for military-grade applications and does not adequately address the scalability and energy-efficiency concerns of consensus mechanisms in such sensitive environments. Most current systems overlook the potential of combining decentralized technologies like LoRaWAN and the Helium Network to ensure secure, long-range communication. Moreover, conventional blockchain implementations tend to use consensus algorithms such as Proof of Work (PoW) or Proof of Stake (PoS), which are either computationally intensive or unsuitable for low-power industrial setups. This study fills the gap by proposing a compact and secure blockchain framework, introducing a novel energy-efficient Proof of Authority (PoA)-based decision technique, and demonstrating its relevance to smart industrial environments and military applications through realistic testing.

3. Proposed Proof of Authority

A family of BFT algorithms designated as Proof of Authority is a governed or permissioned agreement system that seeks to connect a consortium by the use of permitted nodes or validators. The validators have restrictions to sealers that consist of a specific collection of n granted nodes. This protocol's functionality can be summarized up as described below: the validating machines supply the new transaction blocks the fact that the network needs to add. In the following paragraphs, discuss the effectiveness of the preferred framework will be assessed in relation to IoT operations. Building a distributed, decentralized framework for trust is possible with the help of block chain technology. The consensus method, however, consumes a lot of energy, which prevents it from working to its full potential in an IoT service paradigm. IoT, one way to resolve the inconsistencies is to incentivize miners to buy or rent resources from IoT firms. Game theory is used to manage the interaction between IoT service providers and miners in block chain applications based on IoT, and the Alternating Direction Method of Multipliers is used to accomplish distributed and quick proof of work.

- Dynamism of the Network: Considering the PoA framework heavily depends on the sealer's reputation, the network's liveliness indicate that its reputation system does not offer an alternative way for access to a state.
- Tolerance: A maximum of p nodes in a building chain connection with n sealers where,

$$p < \frac{n}{2} \quad (1)$$

As a result, you deploy n nodes to get past this byzantine consensus problem. Although n − p nodes are required to be open and honest, they should all converge at the exact same source of truth, meaning is a distinctive block the inside the network. The validating node or sealers in a PoA-based block chain network should be encouraged to keep up their reputation or strengthen it as a result, since this will restrict the sealers from associating with any detrimental activity on the network.

On comparing between the two in N participant system, Clique just requires N/2 majority or honest participants but IBFT requires 2N/3 participants which guarantees the former more liveness but also drawbacks on more forks are shown in Table 1. Aura functions similar to Clique but for each block creation, it operates in three rounds like block proposal, block acceptance and finally accepted.

Table 1 - Proof of Authority Consensus protocols.

Property	Clique	Aura	IBFT 3.0
Client	Geth, Besu	Parity	Besu
Fork frequency	Prone to more forks	Less forks	No forks
Fork Resolution	Eventual	No guarantee	No forks
Block finality	No immediate	No immediate	immediate
Transaction speed	High	Low	Lesser than clique

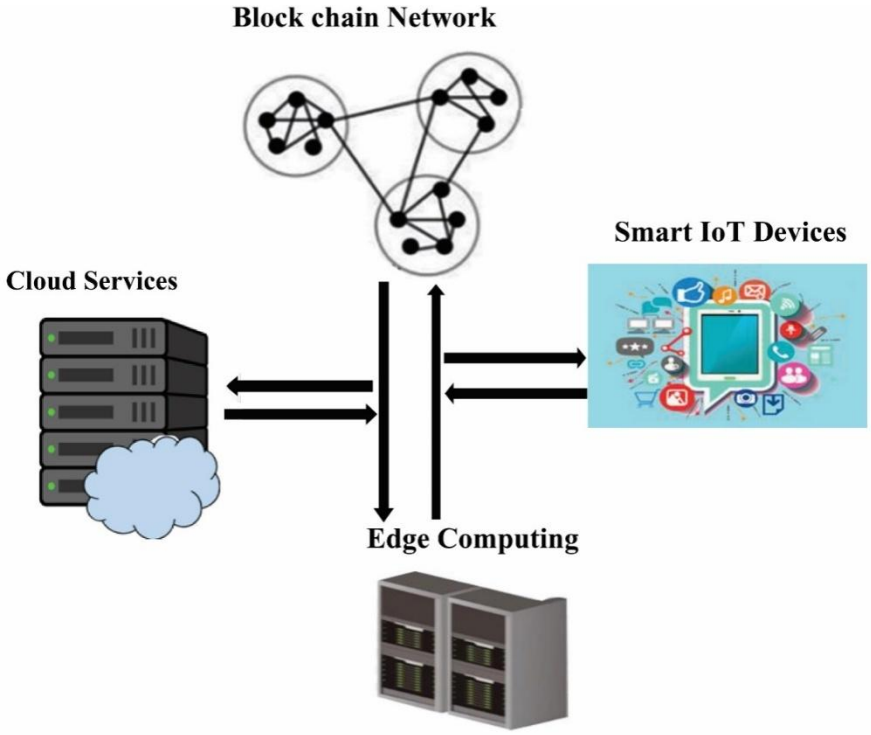

Fig. 1. Architecture of block chain-based internet of things framework.

Future Internet of Things programs' architecture, likely will use an arrangement based on the block chain technology, cloud computing, and edge computing. This architecture might be used to identify and prevent security attacks is shown in Fig. 1. The IoT service framework has the benefit of being quick to identify assaults against identity.

Trust IoT integration of block chain is depicted in Fig. 2. This study only examined two fundamental models and performed a restricted number of performance tests. Block chain integration as part of a trust management strategy to lessen the misuse and exploitation of IoT devices. The new approach proved successful in managing the stakeholder trust relationships in the IoT system, resulting in a more secure setting for IoT traffic management. The authors used time, length, and cost to validate the model.

S1.RK = n(s) denotes the median time taken to respond. R2weeks 1min (Ox13...) is shown to be accurate, for example, when the average response time for services over the previous two weeks was less than a minute. By running a query on the block chain down below, this may be assessed. The constraint for this service will be met if,

$$ri<1 \text{ min} \quad (2)$$

Where the service is ri. Timing of the Ox13 answer. S2. CK = n (s, events) denotes the number of events that are counted inside a certain window. For instance, C3h 2(0x13..., "error") is assessed as true if there have been fewer than two errors in the last 3.h. The service where adheres to the restriction.

$$ei/12<5 \quad (3)$$

Where ei denotes the event's ith instance, service error Ox13.

S3. The list of common occurrences over a precise time period h inside a specific time frame K = V, where h = n. For instance, if there were less than 5 service issues in the preceding 12 hours, the formula V 12h, 1 h 5 is considered to be accurate. The service is able to perform the task.

$$\Sigma_{i=1}ei/12<5 \quad (4)$$

Where ei represents the ith error occurrence of service Ox13 and j is an integer between 1 and (K/h).

S4. The greatest number of events that may have occurred inside a specific time window K during an amount of time h is added to produce the outcome MK,h = n. For example, M12h, 1h

5 is found to be true where the highest number of service errors for each 1-h period throughout the course of the previous 12 h is less than 5. The task can be completed by the service if,

$$ei < 5 \quad (5)$$

Where ei represents the ith error occurrence for service Ox13 and j is an integer between 1 and K. The actions that are recorded in the ledger satisfy S2-S4, but S1 is satisfied by the actions that are added to the ledger using line 8 of listing 1. In this instance, only S1–S4 are used; the others have no bearing on S1.

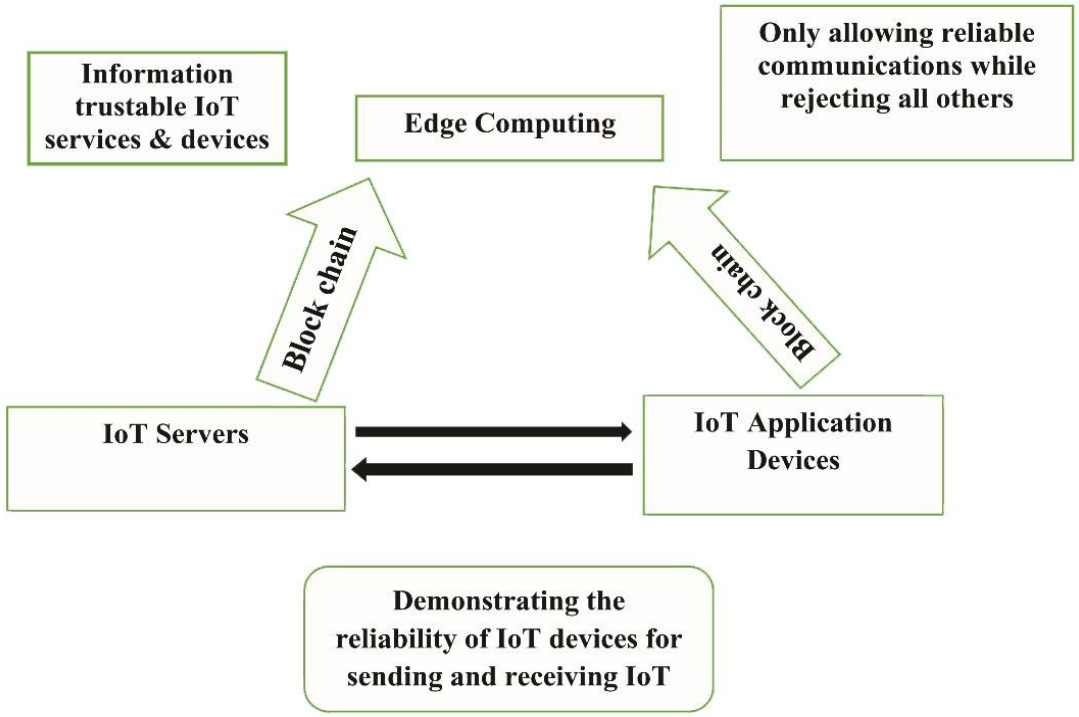

Fig. 2. Trust IoT Integration of Block chain.

3.1. Block Chain

Cryptography is used in block chain technology, a branch of distributed ledger technology, in order to decentralize the control of transaction data. A distributed ledger that is append-only can be used to describe block chains more simply. There is no single entity in charge of the data. Node in the network, each independently verifies a collection of data contained in a block. The block chain is dispersed. It is simpler than conventional centralized systems since it enables a range of peers to join the network without registration. Block chain is an independent system. Block chain introduces trust into the system through a consensus method. A Bitcoin transfer is an image that has the sender, the recipient of the gift amount, and signature on it. Multiple transactions may be contained within only one block, and the phrase "block chain" explicitly encompasses the data structure of Bitcoin. Every block, with the notable exception of the genesis block, which is the first block, remains linked to its precursor by employing the hash of that precursor. Blocks linked to each other preserve the integrity of the block, and each block maintains the Merkle root hash of the transactions to prevent manipulating it.

3.2. Internet of Things

Government entities are attentively tracking the IoT and blockchain convergence. The block chain protocol was initially developed from the Department of Homeland Security (DHS) to handle Network of Things sensors in critical infrastructures. It makes a commitment to deliver programs that may help other departments in mastering block chain technology. The block data project presents several assessment activities for the use of block chains in armed forces industries, such as Network of Things. But no additional details have been given. It indicates from

other official documents and funded by the government study initiatives that defense domains are still discontinuing block chain applications related to the global Web of Things.

3.3. Performance Analysis

The creation of a device-level block chain network architecture implementation is the study's most significant component. Researchers actively assess the four M series processors' asymmetric cryptography capacities. They employed block chain technology in the present research. It has been validated for application in industry by the Validation Programmed with the objective to deliver trustworthy internet of things applications. Equations (5) through (7) can be used to determine the mean (X), standard deviation (X), and standard error (X) of the outcomes that were obtained (Xi) everywhere the whole number of executions (N).

$$X\hat{}=1/N\Sigma_{i=1}X_i \quad (6)$$

$$\sigma_x= \ 1/N\Sigma_{i=1}(Xi-X\hat{})^2 \quad (7)$$

$$\sigma_x=1/N\sigma_x \quad (8)$$

When evaluating the M series CPUs' performance, three performance factors should be considered.

3.4. Comparison with Proof of Work

Another consensus technique adopted in several block chain networks and cryptocurrencies that include bitcoin is Proof of Work (PoW). This consensus model stipulates that generating new blocks in the block chain network involves certain quantities of manpower or computational horsepower. These protections are intended to stop any harmful behavior on the network and lessen the likelihood of to future intrusions. Before a new block is added to the network using a PoW-based protocol, mining nodes must compete to solve an unknown, difficult mathematical equation and get a result that's less than the target number. Additionally, PoA makes it simple to create and sustain applications that are decentralized, all while a centralized approach reduces the number of forks, and thus decreases the number of possible attacks on the network.

3.5. Comparison with Proof of Stake

A sort of mechanism for consensus called Proof of Stake (PoS) was first created as a cost-effective substitute with Proof of Work (PoW). Depending to their stakes in the block chain chain—that is, the number of digital tokens each node in the network owns—PoS leaders are established. In accordance to this the framework the validator node that adds new blocks to the network will be selected in a pseudorandom method. Among N contributing nodes, the probability pi for each node i would be designated as a leader or validator node has been calculated by:

$$p_i = \frac{s_i}{\sum_{j=1}^{N} s_j} \quad (9)$$

(Where si is the node's stake in i). For the objective of adding new blocks to the network, PoA, on one hand, is a reputation-based compromise buildings that depends on only a handful of validating nodes. PoA focuses a higher value on validating nodes' credibility than on their network stakes.

4. Military Application of Lorawan and Helium Network

Whether in a time during war or peace, the military depends upon information and necessitates that it be handed over rapidly. By developing an Internet of Things ecosystem that has been backed by or based after the Helium Block chain, the United States Department of War can open floodgates to get vital information that might not otherwise be hard to obtain. The following are the three primary applications of LoRaWAN IoT devices employed by the DoD.

- Environmental Sensing: There is documented example of timely and trustworthy environmental data collection, such as early earthquake detection and monitoring and real-time urban flood monitoring. By employing this technology, environmental parameters and natural disaster precursor occasions might be watched in real-time, which could help the DoD with arranging evacuations in time for the event. The United States Department of Defense (DoD) may effectively evacuate US ordinary people in advance of lethal

catastrophic events like wildfires, tornadoes, floods, and earthquakes that harm DoD assets with the additional cognitive ability capacity.

- Real-Time Tactical Information: The long-range attributes of LoRaWAN allow IoT devices to be placed in multiple locations and on multiple assets such as personnel, vehicles, and buildings to receive, transmit, and verify data. Since there are normally no reliable sources of Ethernet in deployed or training locations, a satellite uplink would be necessary to manage the Internet uplink for these devices.
- Special consideration must be had when implementing ruggedized LoRaWAN devices in the field as they have a risk of being lost, captured, or reverse-engineered by hostile groups. A ruggedized LoRaWAN device would need obfuscated hardware and software modules to discourage and frustrate any reverse-engineering attempts.
- Critical Infrastructure: LoRaWAN's wireless signal range and broad support of multiple devices could prove to be effective in streamlining the monitoring of critical infrastructure such as electricity, natural gas, water, and sewage. One such example utilizes LoRaWAN for smart infrastructure to monitor physical access to city sewer systems to increase civic response shown in Fig.3.

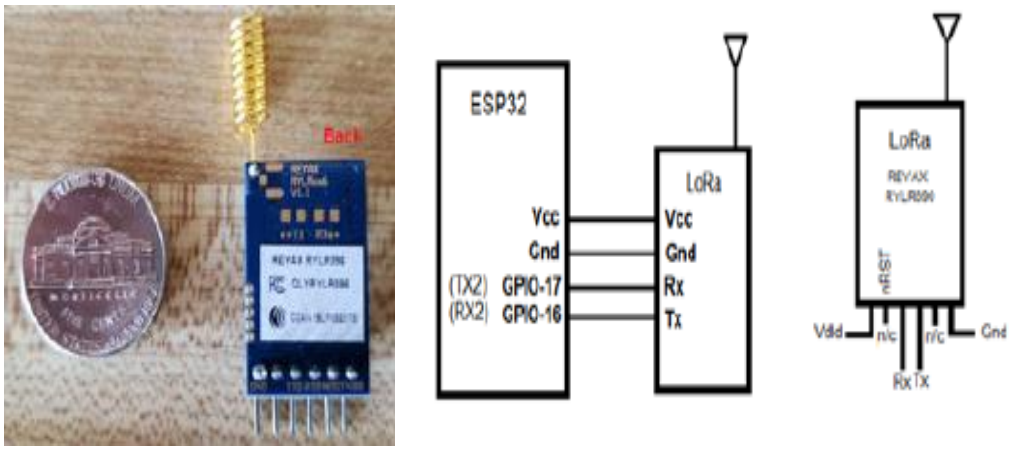

Fig. 3. REYAX RYLR890 Radio Module and Pin-Out Diagram.

5. Use Cases for Block Chain-Based IoT in Military Applications

Use of Block Chain in Missile Defense System: Today let's consider a scenario in which a missile defense system based on blocks could possibly be put to use. In order to understand the potential uses of block chains, one must be familiar with the current missile defense system in play in most military installations, demonstrated in Fig. 4.

- Current Standardized Missile Defense Architecture: Numerous sensors will be acquiring signal data as well as keeping track on both neighboring and enemy airspace. The command-and-control center obtains information on every opponent's aircraft that can be picked up by any one sensor.
- Block chain-based missile defense system: Once a sensor in a missile defense system utilizes block chain algorithms to detect an enemy aircraft crossing the airspace, it alerts the central command and control center of the breach. The communication has been signed electronically and encrypted.
- Employing Block Chain Technology for Coordinating Military Logistics: The positive benefits of block chain technology in military logistical and supply chains lead to guaranteed military items delivery, safety and traceability, and cheaper rates. The military depends its functioning on the efficient assistance of its logistics, which consists of both its supply of human resources and warfighting reserves.

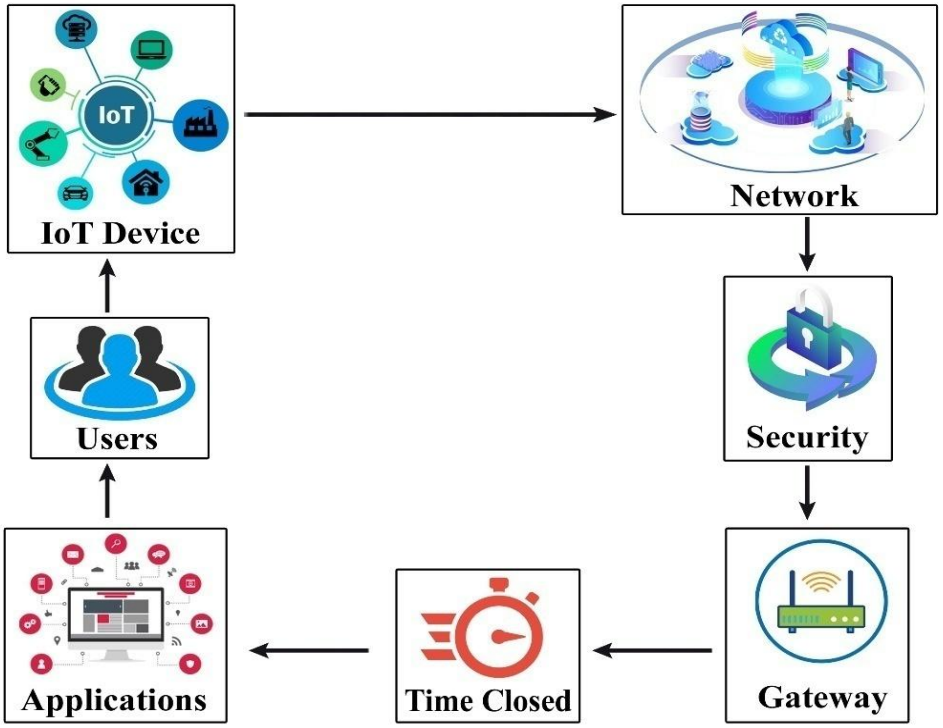

Fig. 4. High-Level scheme of IoT main components.

6. Result and Discussion

The following requirements are considered in relation to the performance of the result: IoT has established itself as a mainstay of current research trends in business and academia. For industrial environments to function better and have greater capabilities, some researchers have developed intelligent systems. Security and privacy, along with other current industry traits, are crucial elements. In this context, a processing architecture built on a block chain was introduced.

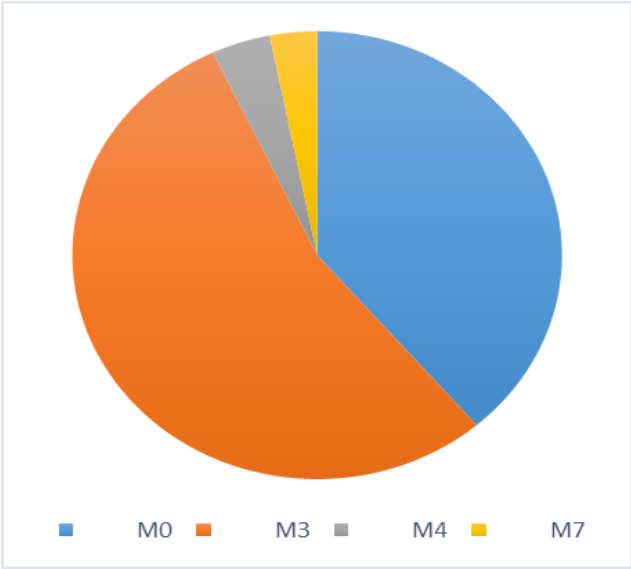

Fig. 5. Performance comparison of execution time.

Table. 2, displays specific numerical data of electricity consumption. This comparison demonstrates that all of the processors have minimal power usage. As a result, implementing trustworthy IoT service operation on block chain processors is a solution that uses less energy. A

solution that uses less energy is to implement trustworthy IoT service operation on block chain processors.

Table 2 - Performance execution time comparison.

Processor	X^(s)	σ_x(s)	σ_x(s)
M0	18.355	0.445	0.085
M3	25.744	0.044	0.575
M4	1.847	0.344	0.759
M7	1.475	0.404	0.568

The power consumption metrics for the various CPUs (M0, M3, M4, M7) are compared in Table 3 and Fig 6. This apparent paradox implies that M7 completes tasks faster, lowering the time it spends consuming power. Higher power consumption over shorter periods of time can lead to lower overall energy consumption than slower processors with lower power draws over longer execution periods since energy consumption is a function of both power and time. It specifically calls into question whether the reported outcomes such as the M7 CPU exhibiting both high average power consumption and possibly the lowest energy use because of its shorter execution time are in line with previous studies in the field. Previous research may have revealed that computers with higher performance consume more power but accomplish jobs faster, resulting in more efficient energy utilization overall. If the current findings support this trend, they are consistent with previous information. However, if the data reveals an unexpected pattern, such as a lower-performance processor utilizing more energy, it may contradict earlier beliefs or reveal fresh insights about processor efficiency. The findings indicate that employing high-performance, energy-efficient processors such as the M7 can considerably improve the responsiveness and battery life of blockchain-based IoT devices. This allows for safe, real-time data processing with low energy overhead, making systems more scalable and practical.

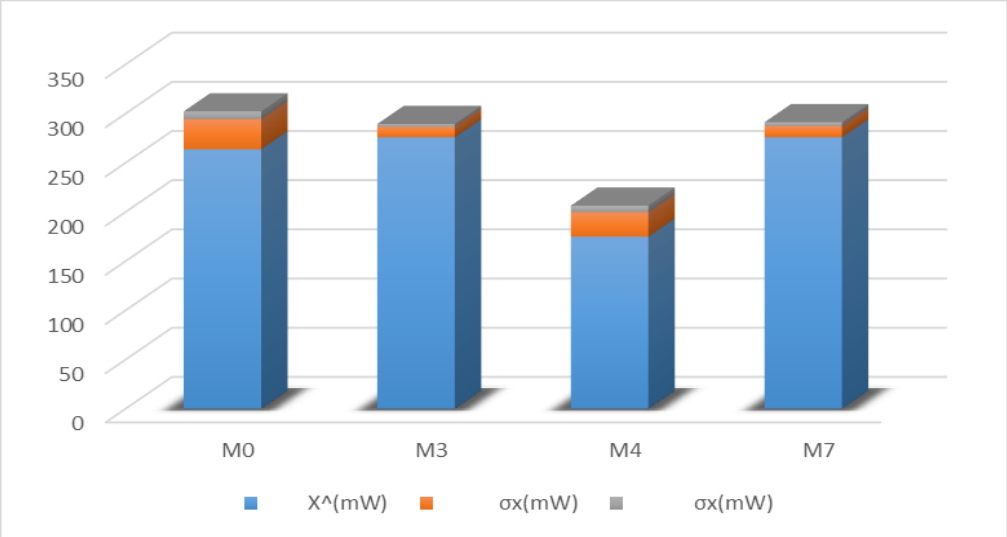

Fig. 6. Detailed comparison of power consumption.

Table 3. Detailed power consumption comparison.

Processor	X^(mW)	σ_x(mW)	σ_x(mW)
M0	263.756	30.674	7.837
M3	275.875	10.746	2.837
M4	174.874	24.847	6.738
M7	275.847	11.474	3.892

Based on the review in the Table.4 of these existing works, this proposed method tries to establish a secure system for data sharing, leveraging POA to ensure data privacy and harnessing block chain in built characteristics to secure data integrity.

Table 4 - Comparison of POA with POW AND POS.

	Proof of Work	Proof of Stake	Proof of Authority
Speed	Slow	Average	Fast
Power consumption	Inefficient	Efficient	Efficient
Security	Permission less, untrusted	Permission less, untrusted	Permission less, trusted
Maturity	Tested	Untested	Safe
Cost	Costly	Less cost	No cost

6. Conclusion

By embracing cutting-edge technologies, the industrial Internet of things enhances smart industries. In order to enhance its lethality and information supremacy, the DoD may be able to overcome IoT difficulties through the use of an exclusive combination of LoRaWAN and Helium Network technology. Block chain's distinctive equipment received attention from both academia and business. An improved degree of automation, security, immutability, trust, decentralized management, and decentralization are just a few of the numerous fundamental properties that block chain technology offers to the smart enterprise. Cyber dangers are inherent with the recent development of digital innovation in military and social infrastructure. One of the newest technologies for defense and security is block chain technology. PoA is a consensus procedure that disregards decentralization in favor of fast throughput and scalability. As such, it is an excellent match for notary-based applications, private block chains, and DApp development and maintenance which depend upon user trust in validators. However, this remains unproven for public block chain networks, such as digital currencies networks, which demand decentralization. However, this construct's performance and cost-effectiveness make it a viable substitute for popular consensus algorithms and an underdeveloped country block chain solution for networks that are private or permissioned. Because a block chain is decentralized, it ensures the integrity of data processing. It makes an important contribution in protecting the system's reliability from online attacks. We provided an overview of the field and discussed current developments in block chain research and development. We also touched about how the Internet of Things uses block chain technology to provide privacy, immutability, and a dependable environment. To allow for effective communication between different devices, a general model for the block chain-based Internet of Things has been developed. This paper proposes an IoT service architecture for intelligent businesses based on block chain technology. The suggested plan makes it possible to create a private, decentralized, secure, and lightweight IoT network that runs on block chain technology and handles important including device and user application, data storage, and the system's functioning. In particular, we present a device-level approach that lowers computing complexity and boosts industrial platform security. Several performance characteristics are taken into account when assessing the performance of the suggested architecture. We also focused concerning the way the Internet of Things uses the technology of block chain to give users privacy, immutability, and an accurate environment. LoRaWAN and Helium Network technologies have a lot to offer the Department of Defense (DoD). They may be used to build smart military bases, save more lives, and monitor the country's vital infrastructure economically.

Acknowledgement

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

References

Ahmad, R. W., Hasan, H., Yaqoob, I., Salah, K., Jayaraman, R., & Omar, M. (2021). Blockchain for aerospace and defense: Opportunities and open research challenges. *Computers & Industrial Engineering, 151,* 106982. https://doi.org/10.1016/j.cie.2020.106982

Akter, R., Golam, M., Doan, V. S., Lee, J. M., & Kim, D. S. (2022). Iomt-net: Blockchain-integrated unauthorized uav localization using lightweight convolution neural network for internet of military things. *IEEE Internet of Things Journal*, *10*(8), 6634-6651. https://doi.org/10.1109/JIOT.2022.3176310

Aseri, V., Chowdhary, H., Chaudhary, N. K., Pandey, S. K., & Kumar, V. (2024). Revolutionizing military technology: How the fusion of BlockChain and quantum computing is driving in defense application. In *Sustainable security practices using blockchain, quantum and post-quantum technologies for real time applications* (pp. 193-203). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-0088-2_10

Ayan, B., Güner, E., & Son-Turan, S. (2022). Blockchain technology and sustainability in supply chains and a closer look at different industries: A mixed method approach. *Logistics*, *6*(4), 85. https://doi.org/10.3390/logistics6040085

Bataineh, M. R., Mardini, W., Khamayseh, Y. M., & Yassein, M. M. B. (2022). Novel and secure blockchain framework for health applications in IoT. *Ieee Access*, *10*, 14914-14926. https://doi.org/10.1109/ACCESS.2022.3147795

Bhawna, Gupta, P., Rai, P., & Chauhan, A. (2023). Blockchain application in consumer services: A review and future research agenda. *International Journal of Consumer Studies*, *47*(6), 2417-2450. https://doi.org/10.1111/ijcs.12940

Ceccarelli, A., Cinque, M., Esposito, C., Foschini, L., Giannelli, C., & Lollini, P. (2020). FUSION—Fog computing and blockchain for trusted industrial Internet of Things. *IEEE Transactions on Engineering Management*, *69*(6), 2944-2958. https://doi.org/10.1109/TEM.2020.3024105

De Villiers, C., Kuruppu, S., & Dissanayake, D. (2021). A (new) role for business–Promoting the United Nations' Sustainable Development Goals through the internet-of-things and blockchain technology. *Journal of business research*, *131*, 598-609. https://doi.org/10.1016/j.jbusres.2020.11.066

Dhar, S., & Bose, I. (2021). Securing IoT devices using zero trust and blockchain. *Journal of Organizational Computing and Electronic Commerce*, *31*(1), 18-34. https://doi.org/10.1080/10919392.2020.1831870

Galán, J. J., Carrasco, R. A., & LaTorre, A. (2022). Military applications of machine learning: A bibliometric perspective. *Mathematics*, *10*(9), 1397. https://doi.org/10.3390/math10091397

Honar Pajooh, H., Rashid, M., 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

Hope, E. T. (2024). Using relays for utilizing and extending LoRaWAN networks with the use of Altibox LoRaWAN infrastructure for internet of things.

Huo, R., Zeng, S., Di, Y., Cheng, X., Huang, T., Yu, F. R., & Liu, Y. (2022). A blockchain-enabled trusted identifier co-governance architecture for the industrial internet of things. *IEEE Communications Magazine*, *60*(6), 66-72. https://doi.org/10.1109/MCOM.001.2100448

Khan, A. A., Laghari, A. A., Shaikh, Z. A., Dacko-Pikiewicz, Z., & Kot, S. (2022). Internet of Things (IoT) security with blockchain technology: A state-of-the-art review. *IEEE Access*, *10*, 122679-122695. https://doi.org/10.1109/ACCESS.2022.3223370

Krueger, J., & Bergmaier, P. (2024, June). Testing Next-Generation Telemetry Using LoRaWAN On High-Altitude Balloons. In *Academic High Altitude Conference* (Vol. 2024, No. 2). Iowa State University Digital Press. https://doi.org/10.31274/ahac.18022

Latif, S., Idrees, Z., Ahmad, J., Zheng, L., & Zou, Z. (2021). A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. *Journal of Industrial Information Integration*, *21*, 100190. https://doi.org/10.1016/j.jii.2020.100190

Li, W., Wu, J., Cao, J., Chen, N., Zhang, Q., & Buyya, R. (2021). Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. *Journal of Cloud Computing*, *10*(1), 35. https://doi.org/10.1186/s13677-021-00247-5

Mohril, R. S., Solanki, B. S., Lad, B. K., & Kulkarni, M. S. (2021). Blockchain enabled maintenance management framework for military equipment. *IEEE Transactions on Engineering Management*, *69*(6), 3938-3951. https://doi.org/10.1109/TEM.2021.3099437

Mtetwa, N. S., Tarwireyi, P., Sibeko, C. N., Abu-Mahfouz, A., & Adigun, M. (2022). Blockchain-based security model for LoRaWAN firmware updates. *Journal of Sensor and Actuator Networks*, *11*(1), 5. https://doi.org/10.3390/jsan11010005

Pavithran, D., Shaalan, K., Al-Karaki, J. N., & Gawanmeh, A. (2020). Towards building a blockchain framework for IoT. *Cluster Computing*, *23*(3), 2089-2103. https://doi.org/10.1007/s10586-020-03059-5

Pióro, Ł., Sychowiec, J., Kanciak, K., & Zieliński, Z. (2024). Application of attribute-based encryption in military internet of things environment. *Sensors*, *24*(18), 5863. https://doi.org/10.3390/s24185863

Rammouz, V., Khoury, J., Klisura, Đ., Pour, M. S., Pour, M. S., Fachkha, C., & Bou-Harb, E. (2023, June). Helium-based iot devices: Threat analysis and internet-scale exploitations. In *2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (pp. 206-211). IEEE. https://doi.org/10.1109/WiMob58348.2023.10187762

Rathee, G., Sharma, A., Kumar, R., & Iqbal, R. (2019). A secure communicating things network framework for industrial IoT using blockchain technology. *Ad Hoc Networks*, *94*, 101933. https://doi.org/10.1016/j.adhoc.2019.101933

Reyneke, M. A., Reith, M. G., & Mullins, B. E. (2023, March). LoRaWAN & the helium blockchain: A study on military IoT deployment. In *International Conference on Cyber Warfare and Security* (pp. 327-XVI). Academic Conferences International Limited. https://doi.org/10.34190/iccws.18.1.944

Sharma, G., Sharma, D. K., & Kumar, A. (2023). Role of cybersecurity and Blockchain in battlefield of things. *Internet Technology Letters*, *6*(3), e406. https://doi.org/10.1002/itl2.406

Sidorov, M., Khor, J. H., Wong, A. C. H., Lee, Y. Y., & Li, J. (2024). A Lightweight Authentication Scheme for LoRaWAN Nodes Represented as On-Chain Nonfungible Tokens. *IEEE Sensors Journal*, *24*(17), 28222-28232. https://doi.org/10.1109/JSEN.2024.3431432

Singh, R., Dwivedi, A. D., & Srivastava, G. (2020). Internet of things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention. *Sensors*, *20*(14), 3951. https://doi.org/10.3390/s20143951

Sokolović, V. S., & Marković, G. B. (2023). Internet of Things in military applications. *Vojnotehnički glasnik*, *71*(4), 1148-1171. https://doi.org/10.5937/vojtehg71-46785

Suhail, S., Hussain, R., Jurdak, R., & Hong, C. S. (2021). Trustworthy digital twins in the industrial internet of things with blockchain. *IEEE Internet Computing*, *26*(3), 58-67. https://doi.org/10.1109/MIC.2021.3059320

Tenneti, S., Jakhar, R., & Harfoush, K. (2024, January). Reactive Jamming of the Helium Network. In *2024 IEEE 21st Consumer Communications & Networking Conference (CCNC)* (pp. 296-301). IEEE. https://doi.org/10.1109/CCNC51664.2024.10454757

Viriyasitavat, W., Da Xu, L., Bi, Z., & Sapsomboon, A. (2019). New blockchain-based architecture for service interoperations in internet of things. *IEEE Transactions on Computational Social Systems*, *6*(4), 739-748. https://doi.org/10.1109/TCSS.2019.2924442

Wang, C., Cai, Z., & Li, Y. (2022). Sustainable blockchain-based digital twin management architecture for IoT devices. *IEEE Internet of Things Journal*, *10*(8), 6535-6548. https://doi.org/10.1109/JIOT.2022.3153653

Wrona, K., & Jarosz, M. (2019, April). Use of blockchains for secure binding of metadata in military applications of IoT. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)* (pp. 213-218). IEEE. https://doi.org/10.1109/WF-IoT.2019.8767315

Wu, Y., Jin, X., Yang, H., Tu, L., Ye, Y., & Li, S. (2022). Blockchain-Based Internet of Things: Machine Learning Tea Sensing Trusted Traceability System. *Journal of Sensors*, *2022*(1), 8618230. https://doi.org/10.1155/2022/8618230

Xie, L., Ding, Y., Yang, H., & Wang, X. (2019). Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. *Ieee Access*, *7*, 56656-56666. https://doi.org/10.1109/ACCESS.2019.2913682

Yadav, A. K. S., Sivaraju, S. S., Radha, B., Sushith, M., Srithar, S., & Kanchana, M. (2024). Malicious node detection using SVM and secured data storage using blockchain in WSN. *International Journal of System Assurance Engineering and Management*, 1-11. https://doi.org/10.1007/s13198-024-02564-9

Yazdinejad, A., Parizi, R. M., Dehghantanha, A., Karimipour, H., Srivastava, G., & Aledhari, M. (2020). Enabling drones in the internet of things with decentralized blockchain-based security. *IEEE Internet of Things Journal*, *8*(8), 6406-6415. https://doi.org/10.1109/JIOT.2020.3015382

Yu, Y., Li, Y., Tian, J., & Liu, J. (2019). Blockchain-based solutions to security and privacy issues in the internet of things. *IEEE Wireless Communications*, *25*(6), 12-18. https://doi.org/10.1109/MWC.2017.1800116

Zakaret, C., Peladarinos, N., Cheimaras, V., Tserepas, E., Papageorgas, P., Aillerie, M., ... & Agavanakis, K. (2022). Blockchain and secure element, a hybrid approach for secure energy smart meter gateways. *Sensors*, *22*(24), 9664. https://doi.org/10.3390/s22249664

Zhu, Y., Zhang, X., Ju, Z. Y., & Wang, C. C. (2020, April). A study of blockchain technology development and military application prospects. In *Journal of Physics: Conference Series* (Vol. 1507, No. 5, p. 052018). IOP Publishing. https://doi.org/10.1088/1742-6596/1507/5/052018