An Integrated Blockchain and IoT approach to secure IoT Communication: A Review

S.R. Ajitha[1], Dr. G.V. Ramesh Babu[2]
[1]Research Scholar, Dept of Computer Science, SV University, Tirupathi, A.P
[2]Associate Professor, Dept of Computer Science, SV University, Tirupathi, A.P

Abstract- The Internet of Things is no longer just a theory. It is the requirement for time in daily existence. The most well-known use of IoT in daily life is the "smartphone." IoT applications are not just found in smart houses. It covers a wide range of industries and sectors, including public safety, agriculture, and health. Because of its many practical uses, the Internet of Things (IoT) is also sometimes referred as the "Internet of Everything (IoE)." The field of Blockchain research is currently expanding quickly. It is a distributed database that keeps track of continuously expanding lists of records called blocks in order to protect them against alteration and tampering. Each block in the chain is connected to every other block by maintaining the hash code of the block before it. Blockchain enabled IoT refers to the dependable authentication, storing, and sharing of data produced by networked devices through the use of a cryptographically secure digital ledger that guards against data manipulation, falsification, or corruption. Blockchain technology is used to protect, authenticate, and decentralize IoT data in a better manner. This enhances the automation and trustworthiness of IoT-based operations and traceability. By combining these two technologies, security can be enhanced.

Keywords: Blockchain, IoT, Attacks, Framework, Security.

1. INTRODUCTION

The Internet of Things (IoT) is becoming more and more important for creating smart applications. By combining cutting-edge and complex technologies, IoT turns traditional applications into smart applications, which helps to increase productivity and service quality. The problems surrounding the security and privacy of IoT data are growing along with the adaptability of IoT devices. The IoT architecture's smart devices are susceptible to several kinds of security attacks and have limited resources.

A centralized server facilitates communication amongst IoT devices, raising the possibility of a single point of failure. Because there are various security vulnerabilities in every tier of the Internet of Things architecture, it is challenging to create a security model that takes this heterogeneity into account.

Furthermore, the sophistication of security assaults is increasing daily. Malevolent node injection, impersonation, physical attacks, phishing, jamming, and data leakage are a few of the well-known attacks in the Internet of Things architecture. Strong technology is needed to withstand these security breaches. The security system that is intended to detect these types of assaults needs to meet basic requirements including availability, confidentiality, and integrity. Conventional cryptographic approaches cannot provide sufficient security for IoT devices due to their storage capacity is low and energy consumption is high. Considering the constant evolution of security risks in IoT, designing an effective security model is a difficult issue. Blockchain technology are highlighted in this study as a means of guaranteeing the security of IoT data.

1.1. SECURITY THREATS IN IOT

One of the key considerations in the creation of IoT devices is security. All of the sensors and actuators connected to an IoT device will become vulnerable to attack. It is recommended to replace all of the hardware components and sensors in such circumstances. It is not practical to replace the compromised devices in real-time applications due to the high cost and work involved. Creating a security architecture that can get around this restriction with conventional techniques like user authentication, access control, and encryption is difficult. Fig. 1 shows the taxonomy of IoT security threat categories.

Access control, impersonation attacks, eavesdropping attacks, denial of service (DoS) attacks, and routing attacks are the main categories of security concerns in the Internet of Things.

1.1.1. ACCESS CONTROL

Access control pertains to user identification and IoT device authentication. Better access control and maintaining the security of IoT data are difficult due to the heterogeneity of IoT devices. Access control consists of three distinct components like authorization, confidentiality, and authentication.

• Authorization: One of the crucial security factors that grants users access to files, services, application data, and other resources is authorization. IoT device authorization that protects privacy can be achieved through the use of blockchain based authorization mechanisms in the creation of a multi-layered security network.

• Confidentiality: Confidentiality or privacy aids in preserving the privacy of different Blockchain-based apps. To guarantee secrecy, blockchain uses a variety of methods, including tokenization, symmetric encryption, and asymmetric encryption. While asymmetric methods utilize different keys for encryption and decryption, symmetric methods employ the same keys for both processes. Tokenization, on the other hand, transforms the important data into digital tokens that may be used on Blockchain platforms. Symmetric encryption techniques include Rivest Cipher 4 (RC 4), Triple DES, Advanced Encryption Standard (AES), and Data Encryption Standard (DES). Accordingly, asymmetric encryption methods include RSA, Diffie–Hellman, Elliptic curve cryptography (ECC), and Digital Signature Algorithm (DSA).

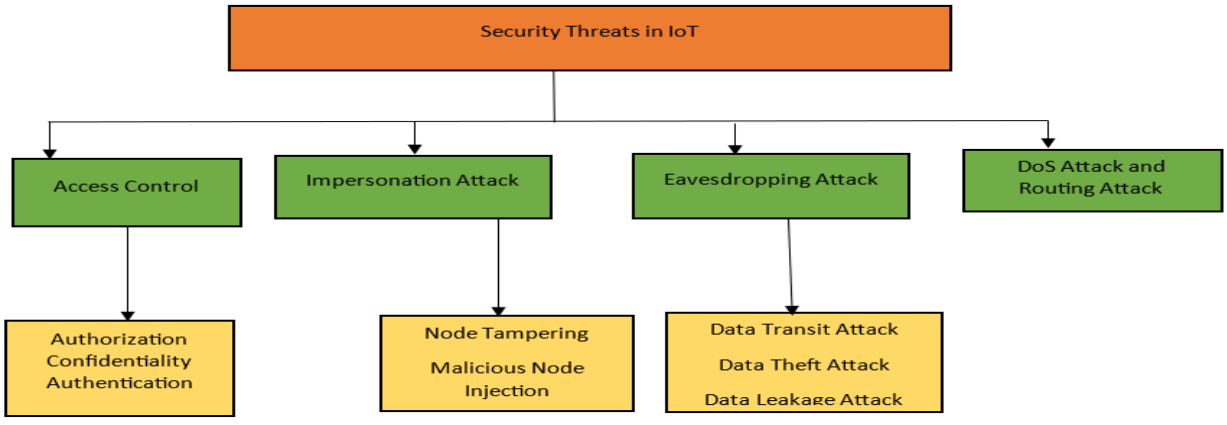
Encryption techniques protect data confidentiality in the Internet of Things by enabling safe communication between two organizations. Even while privacy is protected, there are still risks associated with it. The utilization of Attribute based encryption (ABE) methodologies is regarded as a prospective instrument for enhancing privacy within Blockchain applications.

• Authentication: Since nodes and blocks are checked before a transaction is initiated, the decentralized architecture of Blockchain enables authentication by default. The node is only enabled for the authentication process if it possesses a private key that corresponds to the public key. The Bubble of Trust is a decentralized authentication strategy that is suggested for the purpose of authenticating nodes, as developing a strong centralized authentication solution is somewhat complicated. A ticket is sent to the nodes in this process for authentication, and a private key is used to construct an encrypted object ID that is subsequently used to identify the nodes that have been authenticated.

1.1.2. IMPERSONATION

An impersonation attack happens when a perpetrator assumes a false identity in order to obtain confidential data. There are several ways to introduce impersonation attacks: manipulating the node, introducing a malicious node into the Internet of Things network, or using a Man in the Middle Attack, where the attacker forcibly interrupts and transmits the data shared between two organizations.

• Node Tampering: Node Tampering is an attack in which a physical assault is used to take control of the sensor node. Node tampering typically takes place in the Physical Layer of an IoT system, where attackers alter or take advantage of the real node to replace it with a malicious node. The attacker attempts to obtain unauthorized access to the IoT network by swapping out the compromised node.



• Malicious node injection: The hacker's goal in this attack is to get hacked data into the database by inserting adverse code into the application module. The information-carrying nodes are also compromised as a result of the malicious code injection, which seriously jeopardizes the security and privacy of the Internet of Things system.

• Man in the middle (MiTM) attack: In IoT applications, the most frequent type of assault is the MiTM attack. Spoofing and impersonation attacks are examples of MiTM attacks that cause communication disruptions by hiding the user's identity. As an example, node A tries to contact end-user X while end-user X may be corresponding with the MiTM attackers posing as end-user X. This creates significant security risks because there is more likelihood that the attacker will obtain data leaks.

1.1.3. EAVESDROPPING ATTACK

Here, the attacker uses device spoofing to try and obtain unauthorized access to the network data. Data leakage, data theft, and data transportation attacks can all be caused by eavesdropping.

• Data transit attack: In a data transit attack, the hacker watches the data packets that are dispersed around the network in an effort to find opportunities to exploit them. The two types of data transit attacks that happen most frequently are sniffing and MITM attacks.

• Data theft: An effort to take important information from the Blockchain network is known as data theft. One way to accomplish this is to listen in on conversations that take place between two parties.

• Data Leakage: It involves the disclosure of private information to unaffiliated third parties via a wireless or physical communication route from the Blockchain system. Numerous private pieces of information, including user sensitive data, transactional data, private information, and electronic health records, may be compromised.

1.1.4. DOS ATTACK

DoS attacks are a severe attempt to tamper with, corrupt, or block access to network data by legitimate users. DoS assaults increase a system's susceptibility to security risks, which presents serious difficulties for network security.

Because of its simplistic design and user interface, denial-of-service (DoS) attacks—both single and multiple sources—are easy to plan and cause havoc on a targeted system without requiring a lot of knowledge, skill, or resources to operate. Even though a denial-of-service attack does not result in the loss of critical data, it can seriously impair the system's ability to function.

1.1.5. ROUTING ATTACK

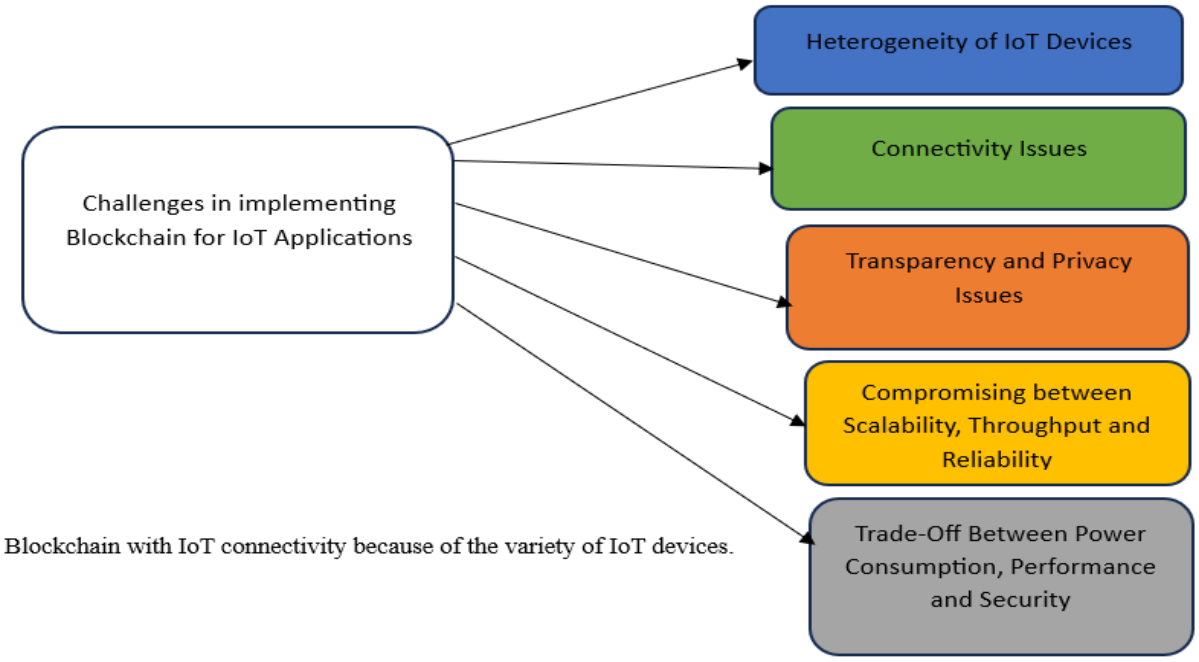
Routing assaults often take place at the network layer, where the perpetrator injects compromised or impacted nodes to alter the communication path's routing during the attack. The perpetrator ruins the whole communication process by changing the routes.

1.2. BLOCKCHAIN FOR IOT SECURITY

As of late, blockchain technology is thought to be among the best in defending against numerous harmful security risks. For Internet of Things applications, blockchain offers a decentralized platform that reduces the possibility of a single point of failure. Blockchain technology often resists the alteration of data. Stated differently, modifications made to one of the ledgers are propagated to all nodes involved in the transaction, and the revised data is recorded in the ledger. It is difficult to change a transaction once it has received authentication from every node in the network without also changing the data in the blocks that came before it.

The unchangeable and irreversible nature of Blockchain is referred to as this. Each block in the network is connected to every other block by a chain, and each block contains the previous block's hash value. Blockchain technology's distributed and decentralized structure, together with its cryptographic features, make it a viable option to tackle the security issues in the Internet of Things. However, due to issues with complexity, high processing costs, throughput, and latency, integrating Blockchain and IoT is difficult. The difficulties that arise when using blockchain technology for IoT are illustrated in Fig. 2 and covered in the points that follow.

• Heterogeneity of IoT devices: A network of tiny sensors and linked objects is used by Internet of Things (IoT) devices to communicate with one another via a variety of communication routes. The integration of IoT with blockchain technology is made more complex and challenging by the heterogeneous and dispersed nature of IoT devices, which make up a network of dissimilar devices. It's difficult to allow



Blockchain with IoT connectivity because of the variety of IoT devices.

• Connectivity Issues: The IoT devices are anticipated to establish connections with various networking systems and disseminate relevant data to relevant parties. Nevertheless, it is challenging to integrate these devices with Blockchain to offer new services and economic prospects in many applications because of their limited storage capacity.

• Transparency and Privacy Issues: Transaction transparency is guaranteed by blockchain technology. However, in the majority of crucial applications—such as banking and healthcare—it compromises customers' privacy and confidentiality when they exchange and access data via IoT equipment. Developing a blockchain-based IoT access control system is crucial to striking the right balance between privacy and transparency.

• Performance, Security, and Power Consumption: The high processing and power needs of blockchain algorithms are often what set them apart. This restricts the usage of Blockchain for resource-constrained applications such as the Internet of Things (IoT) and raises concerns about the effectiveness of Blockchain in processing IoT data. Researchers have suggested refining Blockchain consensus techniques to increase transaction speed and maximize blocks per second. For example, Blockchain performance can be enhanced by eliminating the proof-of-work (PoW) consensus method, which uses less power. However, proof of work (PoW) renders the Blockchain platform immune to malevolent threats and decentralized attacks. This means that there needs to be a reasonable trade-off made between power conversion, performance, and security.

• Scalability, throughput, and reliability: IoT systems have constant data flow, which raises concurrency. The throughput is restricted by the intricacy of Blockchain cryptography, which also impacts the consensus procedures' operational efficiency. In addition, a higher bandwidth is required to boost the throughput due to the more blocks in a chain. It is concerning to think that raising the throughput could compromise the scalability and dependability of Blockchain systems.

2. LITERATURE SURVEY

The proliferation of IoT devices has led to a renewed focus on finding security and privacy solutions for users' data. Similarly, BC technology has become a viable option for communications that are transaction-based and secure. The authors of article [1] demonstrate that unless scalability difficulties are resolved, integration of IoT with BC is not possible. The BC ledger can scale over all peers thanks to the

proposed structure, which establishes a Lpeer network. The implementation testbed's results demonstrate that ledger weight and TPS can both be significantly improved. This will solve the memory requirement issue for storing the blocks and enable improved scalability of large-scale business transactions in the Internet of Things. A portion of the present implementation and assessment was completed on virtual computers, where the application is implemented in node red.

In paper[2] author explained Blockchain's various qualities, including smart contracts, decentralisation, transparency, data immutability, data privacy, and a consensus process, make it suitable for securing data and achieving its integrity from alteration and tampering. This paper proposes a Blockchain strategy to improve agriculture data security, integrity, management and sharing performance. The proposed approach works in three steps, collecting raw agricultural data from greenhouses and storing it in Edge. This data is encrypted and uploaded to InterPlanetary File Systems (IPFS). Then, a transaction is generated by the smart contract and stored in the Blockchain network. The approved transaction cannot be modified. Therefore, our system is guaranteed in terms of security and integrity.

Blockchain is a promising technology towards a transparent supply chain of food, to address secure, reliable and transparent way to ensure food safety and integrity. In paper [3] Sha256 algorithm is used to encrypt the information and the consensus algorithm is used to identify the corrupted chain, pick the correct chain and replace wrong with right chain. PoW is the mathematical puzzle. The node which solves the puzzle first will be miner who gets the reward. The Block Explorer is used to retrieve the block information. The current agri-supply chain management system can be enhanced to implement Agri-Insurance against weather conditions that affect their crops or other risks such as natural calamities. Government Panel can also be included in the Blockchain network to give wise suggestion to the farmers enabling farmers to take fruitful decisions and when the end Consumer scan the QR Code in the product, should be able to trace the entire information about that product.

In Paper[4] author discussed about Directed acyclic graph (DAG) blockchain. It is a new paradigm of blockchain that solves the poor scalability and low throughput caused by a single-chain structure for IoT applications in the blockchain. However, for DAG-structured blockchains, it is difficult to determine the order of blocks. Additionally, there is also lack of secure and efficient ways to generate blocks in parallel. To address these problems, we pro pose an efficient DAG blockchain architecture. First, a novel heaviest chain rule based on the block weight is proposed to guide the selection of the parent and uncle blocks for a new block, which realize that appending is ordering. Second, a tree based gossip protocol (TBGP) is proposed to improve consensus efficiency by reducing message redundancy. Furthermore, feder ated learning is used to select nodes constructing the tree-based gossip network (TBGN). Finally, compared to the random gossip protocol (RGP), the simulation results indicate TBGP can effec tively reduce communication redundancy and improve consensus efficiency.

Blockchain technology has a significant application in smart farming due to its immutability, decentralization and transparency properties. Data exchanged in an Internet of Things (IoT)-based smart agriculture can be used to remotely monitor the fields and regulate the crop needs for optimal productivity. However, such data is sensitive to several attacks, such as man-in the-middle attack, replay attack, ephemeral secret leakage attack, impersonation attack and denial of service (DoS) attack. The existing solutions to counter these attacks are either costly or lack significant security features. To mitigate these issues,author designed a novel lightweight blockchain based authentication scheme based on a fully decentralized and distributed architecture in paper[5]. The designed scheme is subjected to a rigorous security analysis and also a formal security verification using the widely-used Auto mated Validation of Internet Security Protocols and Applications (AVISPA) tool, and it is shown that the scheme is robust and secure against various passive and active attacks. A detailed comparative analysis shows that the proposed scheme has the low communication cost and significantly lower computation cost while satisfying all the security and functionality features as compared to those for other existing relevant schemes.

The Blockchain-SDN integrated architecture provides the security in communication for IoT network. The data transfer from IoT devices is carried out in a secure channel through SDN configurated network layer and secured in a Blockchain model. This proposed model detects the DDoS attack by analyzing the network traffic between the nodes. Thus, the proposed architecture in paper [6] improves the complexity of the system and secures it from DDoS attacks and provides the services to the users efficiently.

Internet of Things (IoT) allows both physical and virtual objects to communicate with each other over a network. The services provided with IoT helps in easing the day-to-day activities. IoT has numerous advantages like scalability and ease of access but the drawback of the IoT system is that a centralized cloud is required for data storage and ensure the security and privacy of the users. In order to eliminate the drawback of IoT, recent studies by author in paper [7] have highlighted the integration of IoT systems with the distributed ledger technologies like Blockchain. The Blockchain technology would provide military grade security to the data. This article presents a comprehensive literature review for the Internet of Things (IoT) and Blockchain protocols.

In paper [8] in author's perspective IoT devices have become a primary medium for malware (e.g., botnets) to launch Distributed Denial of Service (DDoS) attacks. Such malware exploit low-security measures in IoT devices to spread in networks and recruit new victims. Thus, there is a need for malware countermeasures that consider both the security and operability of the network. Indeed, some IoT devices might run critical processes that do not tolerate interruptions. This paper proposes MalCon, a blockchain-based malware containment framework for IoT. It aims to stop malware from spreading in a network by a set of containment strategies encoded into smart contracts to be executed by the infected devices. Moreover, MalCon provides a monitoring service that ensures trustworthy behavior in the network and reports to the system administrator any fraudulent activity of the monitored devices. MalCon was tested extensively with real-life malware and use cases. It quickly and drastically reduces the number of infected devices in a network, even in an extreme case of a fully connected network.

Because of unexpected opponent (malicious) behavior, it may be nearly hard to model highly accurate cyber-attacks on blockchain-based edge networks in real-world scenarios. Today's industrial edge-enabled IoT systems may be able to bolster their defenses against cyberattacks by implementing the unique, distributed blockchain-based security architecture that the author of this study presented in paper [9]. We build a probabilistic model that takes into account

1. hardware level attack
2. network-level attack (IoT, Edge)
3. software-level attack, wallet, smart contract, and
4. blockchain network-level attack in order to estimate the success probability of a malicious attacker on a blockchain-based edge network.

In paper [10] author has discussed about various IoT's fundamental components, including the wireless sensor networks and the internet, have an unsecured foundation that leads to DoS attacks, namely, sinkhole, blackhole, and grey hole attacks. To maintain the integrity and security of the IoT networks, many researchers implemented distributed ledgers in IoT environments. In this paper, we designed a hybrid framework between blockchain and IoT devices, the aim is to secure data transmission in IoT networks using blockchain technology to defend against DoS attacks. Our framework is called HFSDT IoT. The method proposed in this paper consists of two phases to maintain security in the IoT. In the first phase, both a list of attackers and a safe list based on the Ethereum Proof-of Stake (PoS) protocol is used, which complemented by utilizing the proposed IDSs Intrusion Detection System to discover malicious things. In the second phase, to decrease the obstacles in facilitating communication between blockchains, the inter-blockchain communication model creates a network of multiple blockchains with secp256k1 encryption used for heterogeneous blockchains. The experimental results of simulated scenarios show the HFSDT IoT strategy can achieve better results when DoS attacks were launched compared to other blockchain-based methods, namely Bubble of Trust and Credibility Verification Method.

As of today, most of the Internet of Things (IoT) devices work in a centralized environment. With IoT devices having to execute thousands of operations per second, it has become difficult for centralized systems to handle such platforms. Also, factors like operational and maintenance cost of these server machines and danger of DoS(Denial of Service) attack on such servers has threatened the practitioners to come up with a more distributed way of storing the contents. With its decentralized and privacy preserving features, blockchain technology fits well into the scheme of things. This mitigates the quintessential challenges faced in most of the centralized systems. Paper [11] is focusing on the new firmware update scheme to perform the update operations securely. We propose a blockchain based solution for managing firmware updates in IoT. Improper management of devices and distribution of firmware updates from the device vendor could sabotage the IoT ecosystem. The objective of this proposed scheme is to verify and distribute the firmware binaries securely to the IoT device deployed by the device vendor. The PUSH-based method is used for a firmware update in which verification of firmware is done by Hash Chain. It preserves the integrity of firmware by linking the latest version information by previous versions information with the help of a smart contract mechanism.

In paper[12], author combine IoT with blockchain technology and propose a secure and efficient authentication and data-sharing scheme based on blockchain for IoT. We realize reliability and unforgeability of authentication and confidentiality of information. Properties comparisons and performance evaluation indicate that our scheme achieves a proper tradeoff between security and performance com with IoT. Specifically, our scheme Q. Fan et al. is better than the secure and accountable data transmission for IoT based on blockchain in both aspects of security and performance. Compared with Hong et al.'s scheme, the computation cost and communication cost of our scheme are respectively reduced by 15.34% and 40.68%. IoT will lay a foundation in various advanced fields, which may put forward higher security requirements. For instance, anonymity and untraceability of IoT nodes are promising researches. Anonymity ensures that IoT nodes' identities are unknown to malicious entities. Untraceability requires that trails of IoT nodes cannot be obtained by malicious adversaries. We would like to propose an anonymous authentication of IoT to perform more secure data transmission in the following work.

TABLE I THE FINDINGS, LIMITATIONS AND FUTURE SCOPE OF LITERATURE SURVEY PAPERS

TITLE & AUTHOR	ALGORITHM/ TECHNIQUE USED	PERFORMANCE METRICS	LIMITATION(S)	FUTURE SCOPE
1. A Scalable Blockchain Framework for Secure Transactions in IoT, Sujit Biswas	1.Device Registration 2.Device Authorization/Verification	A. Hyperledger Testbed Setup B. TPS Observations C. Block Weight and Ledger Scalability Analysis	IoT and BC cannot be integrated, unless scalability issues are addressed.	Implement the solution in real world situation, and evaluate using real time transactional data.
2. A Blockchain-based approach to securing data in smart agriculture, M'hamed Mancer, Labib Sadek Terrissa, Soheyb Ayad, Hamed Laouz	AES algorithm	Efficiency of Digitalizing Data	Limited data sets	Digitize large data sets and make them available to all the sectors.
3. A Public-blockchain-based De-Centralized Application Framework for Agri Supply Chain Management System, Dayana D.S, Kalpana G	1. Consensus algorithm 2. PoW(Proof of Work) 3.SHA256	Secured Transactions	Blockchain module requires more development efforts	Government Panel can also be included in the Blockchain network to give wise suggestion to the farmers enabling farmers to take fruitful decisions and when the end Consumer scan the QR Code in the product, should be able to trace the

				entire information about that product
4. An Efficient DAG Blockchain Architecture for IoT, Lang Li, Dongyan Huang and Chengyao Zhang	1. Block Graph Generation. 2. Consensus Mechanism.	1.message redundancy 2. choosing the uncle and parent blocks for a new block. 3.Performance.	low system transaction efficiency, low throughput, lack of trust, and security issues with multiparty participation	focus on the problem of improving the accuracy and efficiency of FL for training and constructing TBGN (Tree-Based Gossip Network)
5. Blockchain-Based Lightweight Authentication Protocol for IoT-Enabled Smart Agriculture, Anusha Vangala, Sandip Roy, Ashok Kumar Das.	A novel lightweight blockchain based authentication and key agreement scheme.	communication cost and computation cost	Few existing protocols can guard against attacks	Security and Robustness needs to be improved.
6. Early detection of DDoS attack using integrated SDN-Blockchain architecture for IoT, Dr. A. C. Sumathi, Anchal Ahalawat and Abijoy Rameshkumar.	Integrated Software defined networking (SDN) architecture.	Detect the DDoS attacks	Some instances of the data transfer are executed manually.	Manual execution of data transfer could be automated by constructing a self-sufficient working model, for performance optimization and time complexities. Furthermore, Machine Learning and Artificial Intelligence can be used in the peer-to-peer connectivity between the network nodes in the blockchain to assist with the proof-of-stake (PoS) and proof-of-work (PoW) generation for the block mining and linking it to the blockchain.
7. Implementation of IoT Security System by Incorporating Block Chain Technology, Arepalli Gopi, Nedunuri Madhu Venkata Sai Daswanth, S.S.Aravinth , P.V.Siva Rambabu.	1. Tangle algorithm. 2. PBFT (Practical Byzantine Fault Tolerance) algorithm.	Throughput	Decision making is critical.	Combining other consensus algorithms and comparing throughput percentage.
8. MalCon: A blockchain-based malware containment framework for Internet of Things, Ahmed Lekssaysa, Barbara Carminatib, Elena Ferrarib.	1. Containment smart contract run by privileged peers. 2. Strategies' execution verification procedure run by privileged peers.	1.Security analysis. 2.Performance.	Data sets are not used.	Practical measures to be taken with valid data sets.
9. Estimation of the success probability of a malicious attacker on blockchain-based edge network, Malka N. Halgamuge.	1.Estimation the Success Probability of a Malicious Attacker	Detecting Different types of attacks	Data Sets are not available.	Implementation should be done on valid data sets in order to generate accurate results.
10. A Hybrid Framework for Securing Data Transmission in Internet of Things (IoTs) Environment using	a hybrid method consisting of two phases was proposed for maintaining security in the IoTs	Analysis of detection rate.	Comparing methods are limited.	More accurate methodologies to be considered for better evaluation.

Blockchain Approach, Mohammed Hayman Salih Mohammed.	systems using blockchain technology.			
11. Securing Firmware in Internet of Things using Blockchain, Akshay Pillai, Sindhu M, Lakshmy K V.	Blockchain-based firmware update scheme for the Internet of Things (IoT)	Verification of hash chains.	Downloading binary files of IoT every time is complex process.	Storage needs to be upgraded.
12. A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain, Qing Fana, Jianhua Chena, Lazarus Jegatha Deborahb, Min Luo.	secure and efficient authentication and data sharing scheme based on blockchain for IoT	1.Computational cost 2.Performance 3.Communication cost	Comparison made only in between three schemes.	An anonymous authentication of IoT to perform more secure data transmission in the following work.

CONCLUSION

IoT and Blockchain together have the potential to be quite potent since Blockchain offers attack resistance and trustworthy, auditable peer-to-peer communication. As blockchain technology continues to be incorporated into the Internet of Things, it will bring about profound changes to a number of industries, bringing with it new business models and forcing us to reevaluate how we now operate systems and procedures. The "Blockchain" makes it possible to use Blockchain as a service by facilitating not only the transfer of funds but also the sharing of resources and information among devices. Blockchain technology can be used as a layer in the linked world to provide Security and Communication Attacker stale blocks, enabling a growing number of devices (smart cities, wearables, sensors, IoTs, PCs, smartphones, tablets, and houses) to take advantage of pros. As a result, blockchain offers a lot of exciting prospects for the Internet of Things. Consensus models and transaction verification's computing costs are still issues, nevertheless. Blockchains are still in their infancy, thus these challenges will soon be solved and a plethora of opportunities will become possible.

REFERENCE

[1] *Sujit Biswas, Graduate Student Member, IEEE, Kashif Sharif Boubakr Nour, FanLi, and Yu Wang, A Scalable Blockchain Framework for Secure Transactions in IoT, IEEE INTERNET OF THINGS JOURNAL, JUNE 2019.*

[2] *M'hamed Mancer , Labib Sadek Terrissa, Soheyb Ayad, Hamed Laouz A Blockchain-based approach to securing data in smart agriculture, 2022 International Symposium on innovative Informatics of Biskra (ISNIB),2022.*

[3] *Dayana D.S, Kalpana G, A Public-blockchain-based De-Centralized Application Framework for Agri Supply Chain Management System, 4th International Conference on Smart Systems and Inventive Technology (ICSSIT),2022.*

[4] *Lang Li, Dongyan Huang and Chengyao Zhang, An Efficient DAG Blockchain Architecture for IoT, IEEE INTERNET OF THINGS JOURNAL, 15 JANUARY 2023*

[5] *Anusha Vangala, Sandip Roy, Ashok Kumar Das, Blockchain-Based Lightweight Authentication Protocol for IoT-Enabled Smart Agriculture, international Conference on Cyber-Physical Social Intelligence (ICCSI),2022.*

[6] *Dr. A. C. Sumathi, Anchal Ahalawat and Abijoy Rameshkumar, Early detection of DDoS attack using integrated SDN-Blockchain architecture for IoT, international Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES),2022.*

[7] *Arepalli Gopi, Nedunuri Madhu Venkata Sai Daswanth, S.S.Aravinth , P.V.Siva Rambabu, Implementation of IoT Security System by Incorporating Block Chain Technology, 3rd International Conference on Smart Data Intelligence (ICSMDI),2023.*

[8] *Ahmed Lekssaysa, Barbara Carminatib, Elena Ferrarib, MalCon: A blockchain-based malware containment framework for Internet of Things, Computer Networks 233 (2023) 109853.*

[9] *Malka N. Halgamuge, Estimation of the success probability of a malicious attacker on blockchain-*

based edge network, Computer Networks 219 (2022) 109402.

[10] *Mohammed Hayman Salih Mohammed, A Hybrid Framework for Securing Data Transmission in Internet of Things (IoTs) Environment using Blockchain Approach, IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS),2021.*

[11] *Akshay Pillai, Sindhu M, Lakshmy K V, Securing Firmware in Internet of Things using Blockchain, 5th International Conference on Advanced Computing & Communication Systems (ICACCS),2019.*

[12] *Qing Fana, Jianhua Chena, Lazarus Jegatha Deborahb, Min Luo, A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain, Journal of Systems Architecture 117 (2021).*

[13] *Vinay Gugueoth, Sunitha Safavat Sachin Shetty, Danda Rawat, A Review of IoT Security and Privacy Using Decentralized Blockchain Techniques, Computer Science Review, 50, 1-16, Article 100585, Electrical & Computer Engineering Faculty Publications.*