A Framework (BCsec-DIoT) Using Blockchain Technology and its Applications to Enhance Security within Internet of Thing Systems

Gheithaa Mohammed Saleh[1]; Sira Astour[2]

[1]Master, Faculty of Informatics Engineering Master of Web Science (MWS), Syrian Virtual University (SVU) Syria
[2]Ph.D., Engineering Faculty of Information and Communication Engineering Arab International University (AIU), Syria

[2]ORCID: 0000-0003-3976-9258

Publication Date: 2025/08/13

Abstract: Blockchain (BC) technology has received significant research attention recently because it has decentralization, transparency, and reliable modification as its main distinguishing characteristics, which has made it a fundamental contribution to the development of applications such as cryptocurrencies, healthcare, Internet of Things (IoT) and other fields. IoT devices is envisioned to include billions of deployed mission-critical sensors and actuators connected to the Internet. This network of smart devices is expected to generate and access huge amounts of data, creating unique opportunities for new applications, but critical issues related to security and privacy in IoT environments arise simultaneously because these systems still lack strong security systems. Hence, there was an urgent need to focus on IoT security challenges and take countermeasures. Blockchain offers the advantage of working at both lower and higher levels of communication models, making it a convenient mechanism that can be used effectively across layers and domains. It provides many services such as privacy, security and reliability to systems that rely on it. This research includes a comprehensive analysis and review of blockchain technologies and solutions proposed in academia with methodologies that have been presented for integrating blockchain with IoT, exploring the contributions and challenges that have been included in the literature, also collecting and classifying the types of attacks and threats on IoT and BC. Finally, a framework was proposed that employs Blockchain technology and benefits from its advantages in solving the explored challenges and security problems in IoT systems because it currently provides the most reliable and secure structure file for developing Internet of Things systems by enabling Blockchain technology, consensus algorithm, data encryption and smart contracts to be the algorithm used in this research. Blockchain technology is popular and effective in securing IoT systems over time. In conclusion, this research demonstrates how the integration of BC with IoT can achieve promising results in enhancing the security and privacy within IoT environment.

Keywords: *Blockchain (BC); Decentralized Internet of Things (DIoT); Distributed Ledger; Ethereum; Elliptical Curve Cryptography (ECC); Smart Contract.*

How to Cite: Gheithaa Mohammed Saleh; Sira Astour (2025) A Framework (BCsec-DIoT) Using Blockchain Technology and its Applications to Enhance Security within Internet of Thing Systems. *International Journal of Innovative Science and Research Technology*, 10(8), 195-209. https://doi.org/10.38124/ijisrt/25aug004

I. INTRODUCTION

Our current era is characterized of tremendous technological revolution that has changed the entire world. The current world is witnessing a rebirth of various emerging and modern technologies and fields, such as the Internet of Things (IoT), a field that bears many aspects of development and modernity. IoT devices are currently being widely deployed, and instead of end devices IoT devices are resource-limited devices, unable to secure and defend themselves and easily hacked [1]. Integrating this sector with security technologies will increase the effectiveness of smart and advanced services provided by various devices within the IoT network across various sectors, help protect user privacy and create a secure and reliable environment for storing and exchanging data within these systems [2].

Internet of Things (IoT) represents a groundbreaking shift in how devices interact, communicate and function autonomously across various industries including smart cities, healthcare and wearable technology. Thus, tens or even hundreds of billions of devices will be connected [3]. By enabling devices to gather and analyze data and even make decisions without human intervention, IoT has paved the way for unprecedented technological integration. However, its rapid expansion has revealed significant challenges particularly in security [1]. Many IoT devices are resource-constrained, making them vulnerable to cyberattacks. Ensuring robust security, especially through effective authentication protocols is essential to protect these systems and the sensitive data they handle [2].

The most important issues facing IoT systems are data protection, preventing unauthorized access, modification, or replacement with false or incorrect data [12]. This is a fundamental problem that raises significant concerns, particularly in the fields of personal medicine, wearable devices [13], and many other smart applications where reliability, privacy, and secure access to user data are essential and fundamental requirements that must be secured. Users need a secure and direct means to record, send, and exchange data across networks without any security concerns, quickly and efficiently. The most serious vulnerabilities in the IoT today include weak, easily guessable passwords, insecure update mechanisms, insecure ecosystem interfaces, insecure data, and the transmission, storage, and use of insecure and outdated components. A major reason for poor security is the lack of integrity in IoT systems and the need for these systems' data to be distributed in a way that protects it from tampering, modification, unauthorized access, and other security and reliability issues that need to be achieved [4]. Confidentiality, integrity, and authentication are the pillars of IoT security. Among these, authentication is essential because it verifies the identity of smart devices in the network. If the authentication approach is not sufficiently secured, an adversary can gain control of the network and launch various other types of attacks. Some of the limitations of current IoT environments are [3]:

- Highly proprietary architectures.
- Data integrity/ownership issues.
- Vulnerability to a variety of cyberattacks.
- Single point of failure.
- Unmonitored environments.

There is a need for a decentralized network within which data is distributed to protect IoT systems and applications from many attacks intent on causing damage, sabotage or other purposes. These attacks vary depending on the aspect of the system targeted by these attackers or the gains the attackers seek to achieve from this attack. This, in turn, imposes the need to find effective mechanisms to achieve cybersecurity. Consequently, there are no precisely defined security standards and requirements to prevent such attacks, particularly those related to the reliability and protection of user data during storage, transmission and exchange [5].

To address the Inherent vulnerabilities of centralized IoT systems, a decentralized approach, known as Decentralized IoT (DIoT) has emerged as a vital innovation. Traditional IoT systems rely on centralized servers to collect and manage data which creates potential risks including single points of failure, data breaches and scalability issues [6]. DIoT leverages blockchain technology to distribute control across a network of nodes, enhancing security and reliability while reducing dependence on centralized systems. Through blockchain data is encrypted and stored across multiple nodes making it far more resistant to cyberattacks and ensuring the uninterrupted operation of networks even when individual nodes fail [7].

DIoT advantages are transformative. Decentralization significantly improves scalability, allowing efficient management of vast IoT ecosystems as the number of connected devices continues to grow [8]. Additionally, by automating processes through smart contracts and eliminating intermediaries DIoT systems reduce operational costs particularly in industries that rely heavily on complex supply chains or extensive data management. This decentralized framework not only bolsters security and efficiency but also fosters innovation by creating a more resilient and adaptable IoT ecosystem [9].

Blockchain technology serves as a cornerstone for achieving DIoT's full potential, offering a versatile mechanism for secure and decentralized communication across various layers of IoT systems. By addressing critical challenges like data privacy, scalability and system reliability DIoT represents a paradigm shift in how connected devices are managed [10]. The transition toward decentralized IoT systems is not merely a technical evolution but a fundamental reimagining of IoT's future ensuring it remains secure, efficient and scalable in an increasingly interconnected world. This approach promises to unlock new possibilities from smarter cities to more reliable healthcare solutions reshaping the technological landscape for years to come [11].

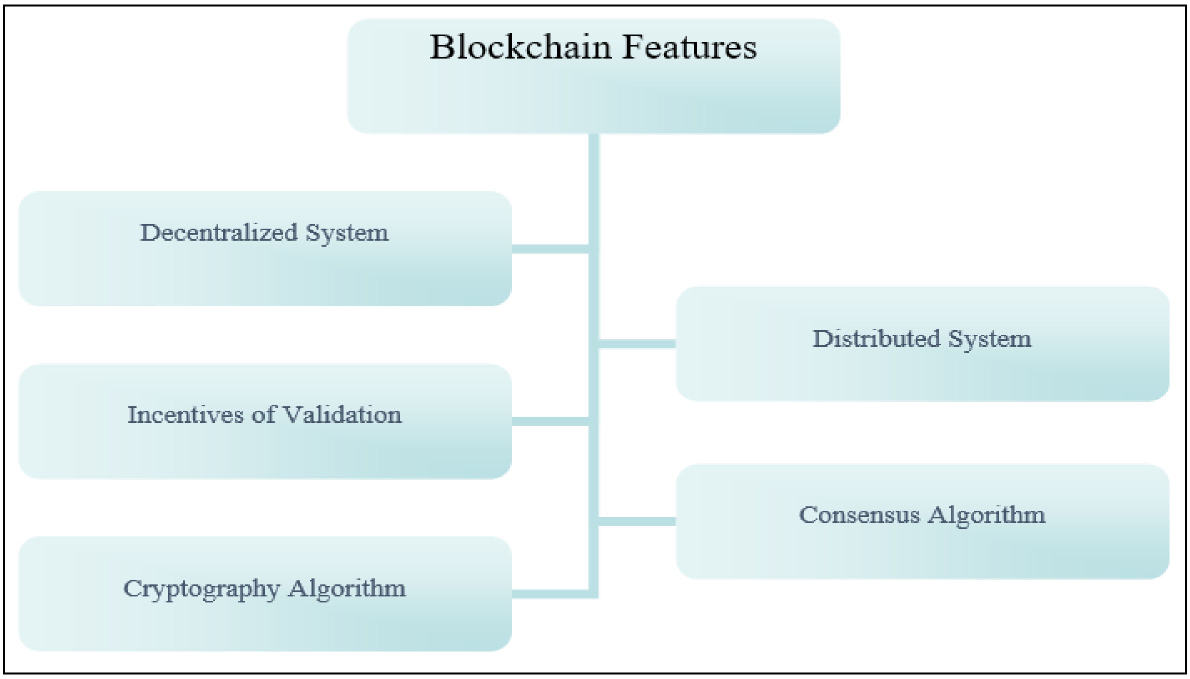


Fig 1 Blockchain Features [14]

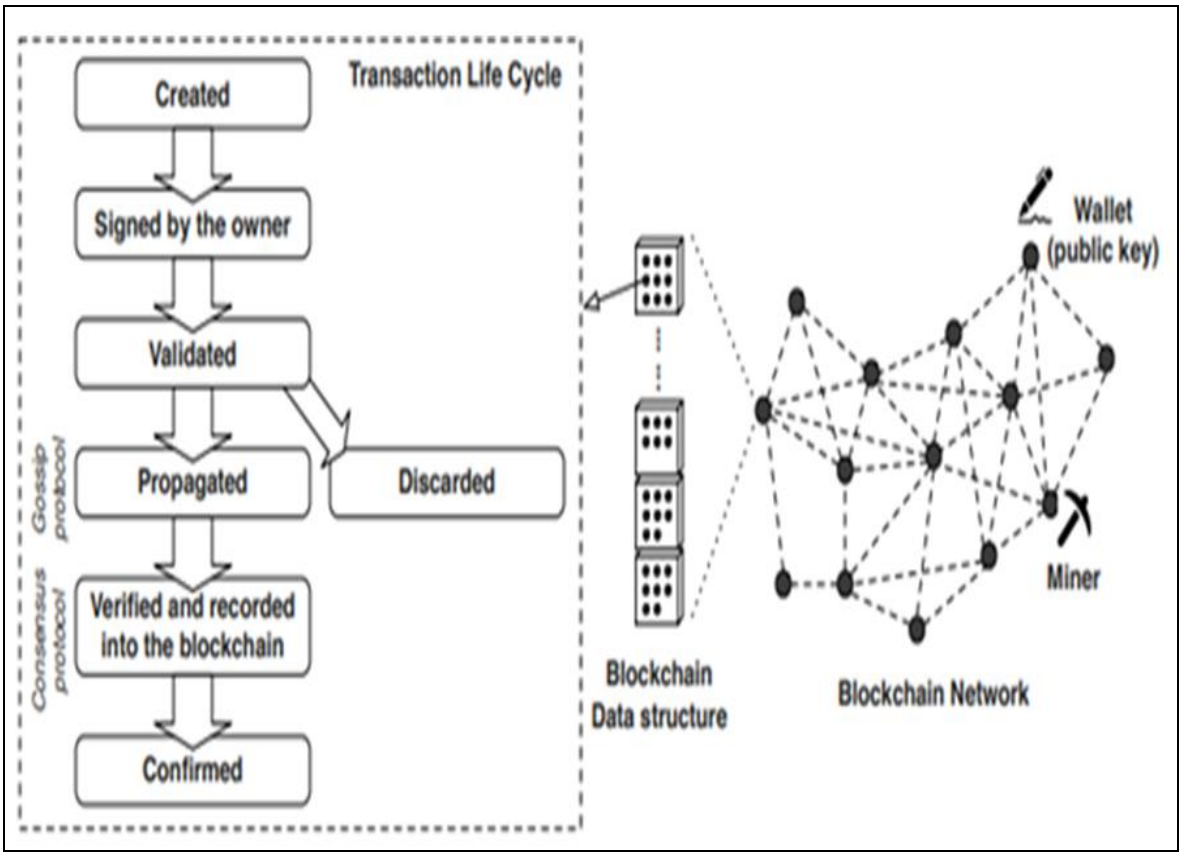


Fig 2 Blockchain Network Structure [15]

Smart contract is a digital contract in the form of a legal contract. It consists of a set of protocols that must be agreed upon by the participating entities under the conditions that lead to the execution of those protocols. In other words, it is a set of cryptographic rules that are only executed if certain conditions are met [16]. Smart contracts have the following characteristics:

- Independence.
- Trust.
- Backup.
- Reducing costs [1].

Smart contracts provide many security features when combined with Blockchain technology. Within the Internet of Things network that uses Blockchain technology (IoT-Blockchain). When smart contracts are introduced into this system, we will obtain a smart network with many features as shown in the figure 3.

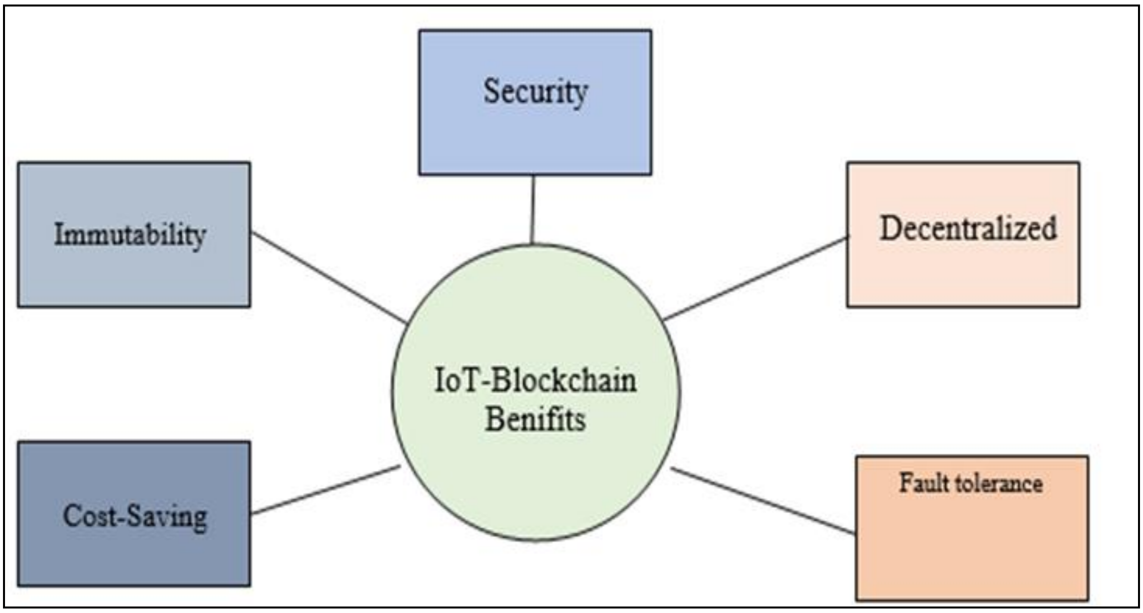


Fig 3 Benefits of IoT-Blockchain Network Using Smart Contracts [6]

Most of the current threats to the Internet of Things can be mitigated through the protection provided by the blockchain. One solution to overcome these issues has been the introduction of Blockchain technology, which will help overcome the security vulnerabilities of IoT.

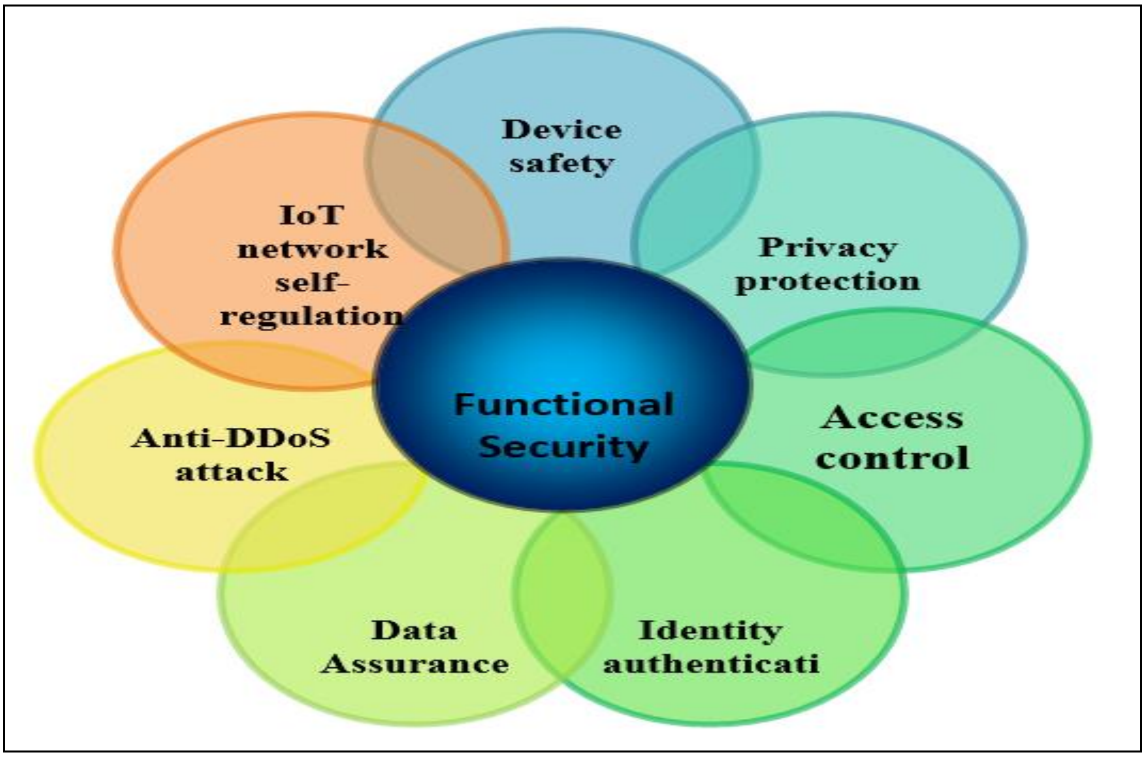


Fig 4 Security Functions Provided by the Application of Blockchain Technology within IOT Systems [17]

II. LITERATURE REVIEW

- *Survey and Review of Related Previous Literature*

In this study [6] Nehemiah Adebayo et al. focused on the security challenges facing Internet of Things (IoT) platforms. They explained that blockchain technology must be implemented in conjunction with other security measures and methods, such as firewalls, encrypted operating systems that can be trusted and software updates that can only be updated through trustworthy sources. They also emphasized that blockchain technology, despite its many advantages, has its drawbacks and may not be ideal for every use case. Furthermore, IoT network devices have limited computing power, storage space and bandwidth; therefore, there is a need to consider other complementary and supportive options. The researchers concluded that IoT security issues can be resolved by enabling blockchain technology, consensus algorithms, data encryption and smart contracts to become the common and effective algorithms used by blockchain technology to secure IoT systems over time. While Bodoor Al-Rayani et al. [1] followed a working approach that initially relied on describing the Internet of Things (IoT) based on blockchain to enhance security through big data processing, ensure data integrity, increase reliability and maintain digital identity privacy without the intervention of a central server or third party. The researchers then demonstrated that one of the outcomes of enabling IoT-Blockchain is the emergence of several advantages that support IoT systems in terms of security and a decentralized ecosystem. The researchers then presented some of the challenges facing IoT-Blockchain, such as scalability and skill shortages, despite its unlimited advantages. This paper then discussed the IoT-based blockchain architecture in general as a five-layered basic framework. It then explained the importance of component-based development CBD in IoT-based Blockchain and how it achieves strong security and privacy goals in detail. The platforms were presented from two aspects, in general and specifically from the SSM component via Google Cloud Platform (GCP). Axel Benjaminsson [7] reviewed the most serious vulnerabilities within IoT systems which are lack of integrity. These vulnerabilities include weak, guessable passwords, insecure data, insecure update mechanisms, insecure ecosystem interfaces and the storage and use of insecure and outdated components. The researcher then explained that most of the current threats to the IoT can be mitigated through the security protection provided by blockchain technology. A large reason for the lack of integrity in IoT systems is that blockchains can provide integrity, authenticity, transparency, decentralization and more. Finally, it has been confirmed that blockchain technology effectively mitigates most of the major threats to the Internet of Things (blockchain will not mitigate weak, guessable passwords, it protects against DDoS attacks and can replace weak authentication systems with public/private key authentication, vulnerable software and dependencies are some of the things that blockchain cannot mitigate, but insecure data transfers and firmware updates can be secured through blockchain transactions) and is therefore considered highly applicable to IoT systems for increased levels of security and reliability. In [18] researchers focused on finding solutions to secure and defend the IoT network from hacking using fog computing and integrating blockchain technology. The researchers demonstrated that fog computing may be more effective than cloud computing in protecting IoT nodes and devices. The approach adopted in this paper is based on a proposed user authentication system using blockchain-enabled fog nodes. These fog nodes interact with Ethereum smart contracts to authenticate users to access IoT devices. While this study [19] discuss the issue of securing trust and identity authentication within Industrial Internet of Things (IIoT) environments. They explain that these environments include devices from different domains collaborating on the same task raising numerous security and privacy concerns regarding device-to-device communication. Secure authentication using blockchain and the BASA key agreement mechanism is proposed for cross-domain IIoT. Specifically, blockchain consortiums are presented as a trusted platform for sharing domain-specific information. Researchers [20] discussed the field of IoT authentication, presented a summary of proposed authentication protocols and compared and evaluated these protocols to identify strengths and weaknesses that should be considered in developing this field. The following evaluation protocols were used: OAuth 2.0, OpenID Connect, TLS, DTLS, and MQTT. The research aims to identify the best protocols for authentication in IoT systems and provide comprehensive information for researchers and developers in this field. This study [21] provides valuable insight into the challenges and opportunities in developing smart vehicle technologies and securing IoT networks. It highlights the importance of using modern and innovative techniques in designing a smart vehicle system using artificial intelligence and vehicle data analysis to diagnose problems and identify their root causes. The importance of security and privacy in IoT networks particularly in authentication mechanisms was discussed. They highlight the challenges in securing authentication and discuss various techniques and assessment schemes for IoT authentication. While this study [4] aims to evaluate the security of Internet of Things (IoT) devices and analyze the security issues, vulnerabilities and open challenges they face. An overview of IoT security and risks is provided, focusing on potential security vulnerabilities and threats. Some existing solutions to address these issues are reviewed, but there are still some open issues that need to be addressed in the future. The researchers also tested some recent techniques for IoT security and came up with some recommendations for future research in this area. Several security solutions for protecting the IoT were reviewed in the research, including encryption of data sent and received via the IoT, the use of security protocols such as SSL/TLS, improved identity and access management for IoT devices, the use of threat detection and response systems and the use of artificial intelligence and machine learning techniques to analyze user behavior and detect threats. Researchers [22] focused on analyzing the security problem of IoT devices and presenting innovative solutions to improve security and protection. The strength of the research lies in providing a comprehensive analysis of the IoT security problem and examining innovative solutions such as blockchain, as well as practical recommendations for improving security and protection. The results indicate that there are several challenges affecting IoT security including identity and access management. Blockchain technology represents a potential solution for enhancing security in the IoT and is used to ensure the authenticity and security of transactions between devices and users. Shalini Dhar et al. [23] proposed a decentralized framework for sharing and exchanging multimedia file systems over a wireless Internet of Things (IoT) network to solve the centralization problem of file sharing systems, where a server or intermediary can be malicious and corrupt the entire data exchange network. Furthermore, sharing multimedia files such as audio, video or large text files across a wireless IoT network is not an easy task, given the complete reliability of other nodes. Blockchain and IPFS were used to provide high security and low latency. Finally, a security analysis of the proposed system was conducted, which proved its robustness in solving most of the security challenges faced by the traditional system. Furthermore, the proposed approach can be applied to any wireless file sharing network (WFS) in the IoT network that requires exchanging multimedia data such as healthcare data, IoT data in wearable devices, traffic data in smart cities and etc. In the approach proposed by Sivaselvan et al. [9], a new blockchain-enabled authentication and access control system for the Internet of Things (IoT) was created. The scheme uses the blockchain as the root of trust. Authentication is performed using a decentralized blockchain-based public key infrastructure (PKI) provided by the scheme. Access control is based on an access token that contains the context and access rights of an IoT device to a specific resource in another IoT device. The scheme stores the information necessary for authentication and access control in the blockchain. The diagram demonstrates resilience to various attack vectors on the Internet of Things (IoT) including repudiation, traceability, key compromise, information disclosure, impersonation, DoS and cluster attacks. Experimental results indicate that transaction costs for all blockchain transactions are well within the recommended threshold. While the approach presented by Asad Ullah Khan et al. [24] is a blockchain-based approach to achieving registration, mutual authentication, data sharing and nonrepudiation within a wireless IoT sensor network. The nodes used in the proposed approach are divided into three types: sensor nodes, cluster heads and coordinators. A consortium-blockchain deployed on the coordinators was used to store the legitimate node identities. Smart contracts were then implemented facilitating the authentication, data sharing and nonrepudiation processes for sensor nodes. Binary node data was stored using the AI-based IPFS (interplanetary file system). The stellar consensus protocol was used. The Stellar Consensus Protocol (SCP) contributed to increased transaction throughput and network efficiency. Finally, experimental tests were conducted on the proposed approach by simulating the execution of transactions on the Ethereum network using an Intel Core-i5 laptop with 6 GB of RAM and a 2.5 GHz CPU core. Smart contracts were created using the Solidity programming language. The web3.py library was used to communicate with users (requester or owner) and smart contracts. Files were stored on IPFS using ipfshttpclient. Simulation results showed that the proposed model's transaction latency was approximately 81.82% lower than the existing proof-of-work model. The approach presented by Mahmoud Tayseer Al Ahmed et al. [10] addressed device authentication on the Internet of Things using blockchain technology. The researchers demonstrated that blockchain authentication models are known to require significant computational resources because they require complex mathematical calculations. Therefore, they introduced the Authentication-Chains protocol, a lightweight protocol. And a distributed blockchain-based IoT authentication provider.

➢ *Analysis of Privious Literatural Review*

- *Solutions Proposed in the Literature to Enhance Security Levels in Internet of Things (IoT) Systems:*

✓ Several authentication protocols have been proposed; these protocols were compared and evaluated to identify strengths and weaknesses that should be considered in developing IoT security.
✓ Fog computing may be more effective than cloud computing in protecting IoT nodes and devices.
✓ Improving IoT security using Physical Unclonable Functions (PUFs). These techniques rely on the unique physical properties of each device and cannot be easily replicated making them ideal for IoT security.
✓ Encrypting data sent and received over the IoT.
✓ Using security protocols such as SSL/TLS.
✓ Improving identity and access management for IoT devices.
✓ Using threat detection and response systems.
✓ Using artificial intelligence and machine learning techniques to analyze user behavior and detect threats.
✓ Introducing new technologies such as quantum computing and improving data identification to ensure privacy.

- *The Most Serious Security Vulnerabilities in Internet of Things (IoT) Systems as Indicated by Previous Literature:*

✓ Weak passwords that can be guessed.
✓ Insecure data.
✓ Insecure update mechanisms.
✓ Insecure ecosystem interfaces.
✓ Storage and use of insecure and outdated components.
✓ The use of physically unclonable functions suffers from limitations related to high cost and difficulty in widespread implementation.

The role and importance of integrating Blockchain technology into Internet of Things (IoT) systems to improve security levels, as indicated in previous literature: The researchers concluded that blockchain technology can solve IoT security problems by enabling blockchain, consensus algorithms, data encryption and smart contracts to become the common and effective algorithms used by blockchain technology to secure IoT systems over time. This will contribute to preserving the privacy of devices and users and their data as we provide an approach to building trust across untrusted domains rather than placing trust in a third party.

➢ *Research Questions*

This research aims to enhance the application of security and reliability standards using blockchain technology on the Internet of Things (IoT) systems. Three related research questions will be addressed:

RQ-1 What are the security challenges and threats within the Internet of Things, and what are the obstacles to achieving a reliable system?

RQ-2 How can blockchain technology be leveraged and employed to build a decentralized, reliable and secure

Internet of Things (IoT) environment that protects user privacy and data?

RQ-3 What are the security benefits of integrating blockchain technology with smart contracts within Internet of Things (IoT) systems?

III. METHODOLOGY

The approach adopted in this research is based on developing a centralized identity and access management system, defining different levels of user access and implementing appropriate security measures to integrate blockchain technology into the IoT. This approach also improves the integration of various technologies within it including smart contracts, distributed ledger, decentralized networks (Ethereum) and programming languages (Solidity and JavaScript) to enhance IoT security and protection.

Relevant research was leveraged, considering all gaps related to trustworthiness, identity authentication, access control and decentralization. We present a security framework that utilizes blockchain technology, smart contracts, appropriate algorithms and techniques which is outperforming existing frameworks in efficiency, achieving higher levels of security and improving safety, a fundamental requirement within any smart IoT system.

In this research we propose a security framework that improves security within IoT systems using blockchain technology which is Blockchain Security over Decentralized IoT (BCsec-DIoT). We implement this security framework to test its effectiveness in achieving security, reliability, access control and identity authentication within Internet of Things applications and networks. This will support the adoption of blockchain technology within these applications to achieve a high degree of security and facilitate the protection of the network and devices from breaches and various types of attacks. This implementation phase includes the following sub-steps:

➢ Using available networks for testing online, such as the Ethereum network, which allows distributed software writing across nodes within the network.

➢ Choosing a platform to work on and writing the implementation code, such as the Remix-Ethereum platform, which enables communication with any Ethereum node.

- *Within the Ethereum Network:*

✓ On the user side the Web3.JS framework will be used with the JavaScript programming language to design a front-end program that allows new users to be added to the IoT network.
✓ On the blockchain side, we will use the Solidity programming language.
✓ By creating a decentralized IoT environment, we will use Blockchain as a data storage location (a decentralized/distributed platform) and a data storage location from which smart devices can take their instructions regardless of the platform used.
✓ Defining specific rules using smart contracts that allow control of devices within the IoT network and writing them in a language that will allow access permissions to these devices and control them by authorized and identified individuals within the system.
✓ Using smart contracts that will enable control of access to data and verify the identity of the person sending a control instruction to a specific device on the network. The instruction is executed based on defined rules that ensure the identity of the person is verified.
✓ Deploying Blockchain within Internet of Things (IoT) systems using Ethereum distributed networks. These Ethereum networks allow software to be written distributed across all nodes within the network using programming language called Solidity which allows for defining specific rules.
✓ Designing encryption algorithms within the contracts to ensure secure communication between nodes and the sink.
✓ Conduct an evaluation of the proposed framework.
✓ Discuss and compare the results.
✓ Propose several suggestions and recommendations for future work.

➢ *Components of BCsec-DIoT Framework*

- A smart access control contract to manage device registration and access control. It defines rules for device registration, authentication, and access control.
- API development using Asp.net to facilitate communication between IoT devices and the blockchain.
- Asp.net: A C# library to interact with the blockchain from the server-side API and process API requests.
- IoT device implementation using Arduino and ESP32 to register and communicate with the blockchain.
- Arduino/ESP32: Hardware platforms for IoT devices.
- Testing and verification: To ensure functionality and security.

➢ *Architecture of BCsec-DIoT Framework*

- *Blockchain layer:* Uses a private blockchain network to manage device identities, authentication, and access control.
- *IoT layer:* Consists of various IoT devices (e.g., sensors, actuators) that communicate with the blockchain to register and transfer data.
- *API layer:* Provides a communication interface between IoT devices and the Blockchain, facilitating device registration and data queries.

IV. MODELING AND ANALYSIS

➢ *General Diagram of The IOT Network*

Figure 5 shows the general diagram of the encryption system used in the IOT network.

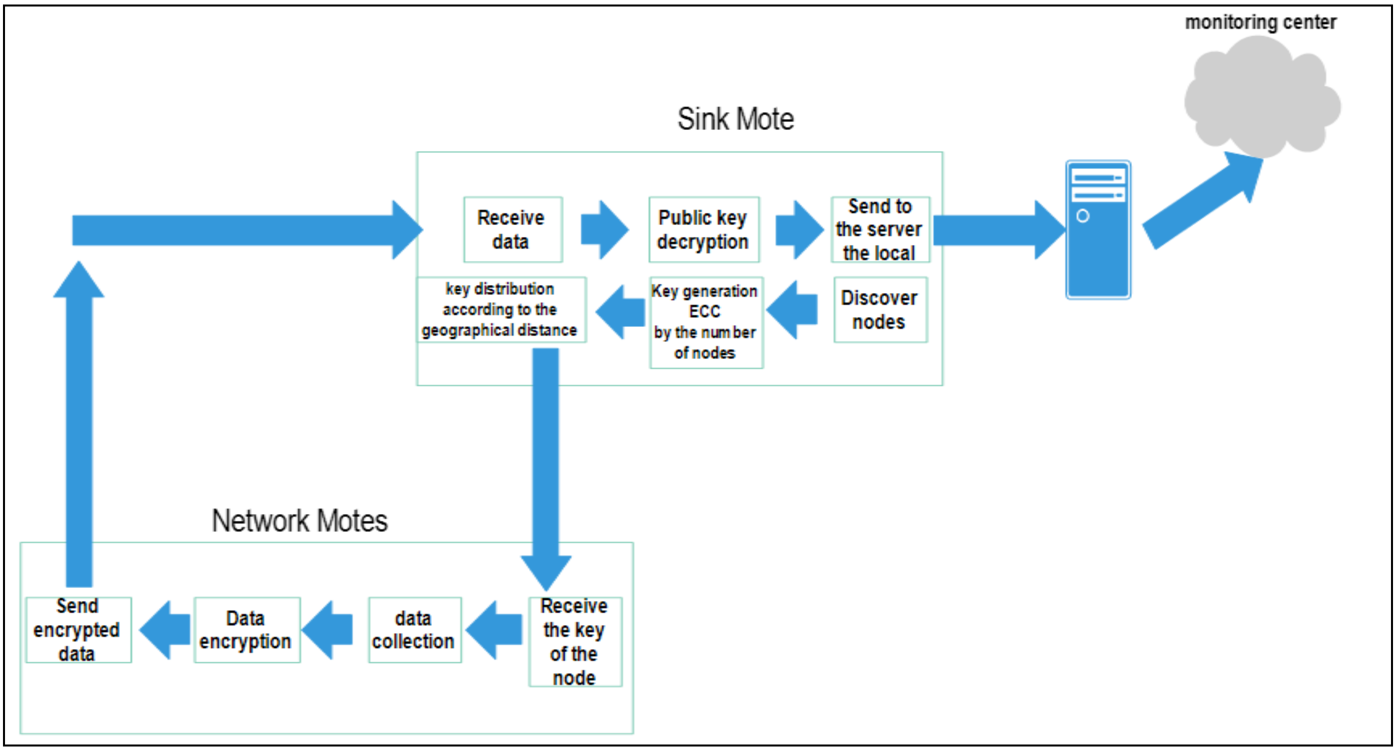

monitoring center
Sink Mote
Receive data
Public key decryption
Send to the server the local
key distribution according to the geographical distance
Key generation ECC by the num ber of nodes
Discover nodes
Network Motes
Send encrypted data
Data encryption
data collection
Receive the key of the node

Fig 5 General Research Flowchart

The aggregator node generates ECC keys for the number of nodes operating in the network and distributes the keys to the nodes, so that each node has its own key. It also obtains the encrypted data and sends it to the monitoring center.

Each node in the network uses its own encryption key to encrypt data using the AES algorithm and sends its data to the aggregator nodes.

The encryption keys are changed periodically, increasing the level of security.

The data is sent to the monitoring center, a website that allows network administrators to monitor network resources.

➢ *Integration with the Blockchain*

Figure 6 illustrates the method for integrating with the Blockchain:

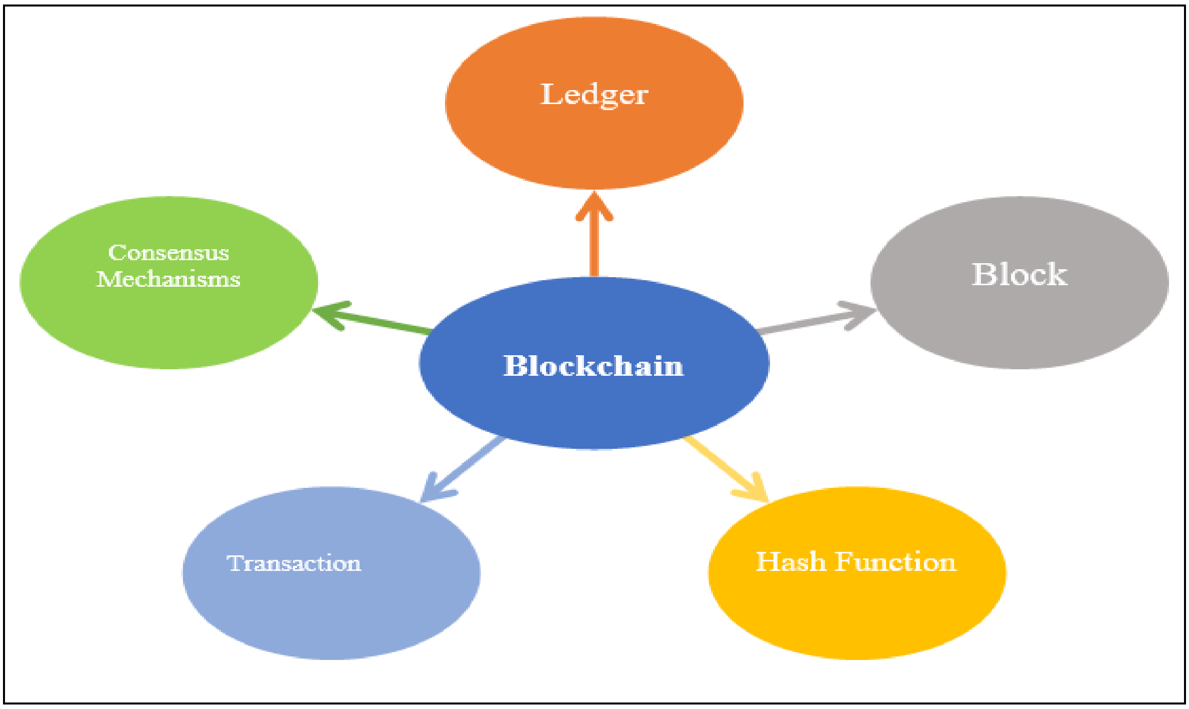


Fig 6 Blockchain Components

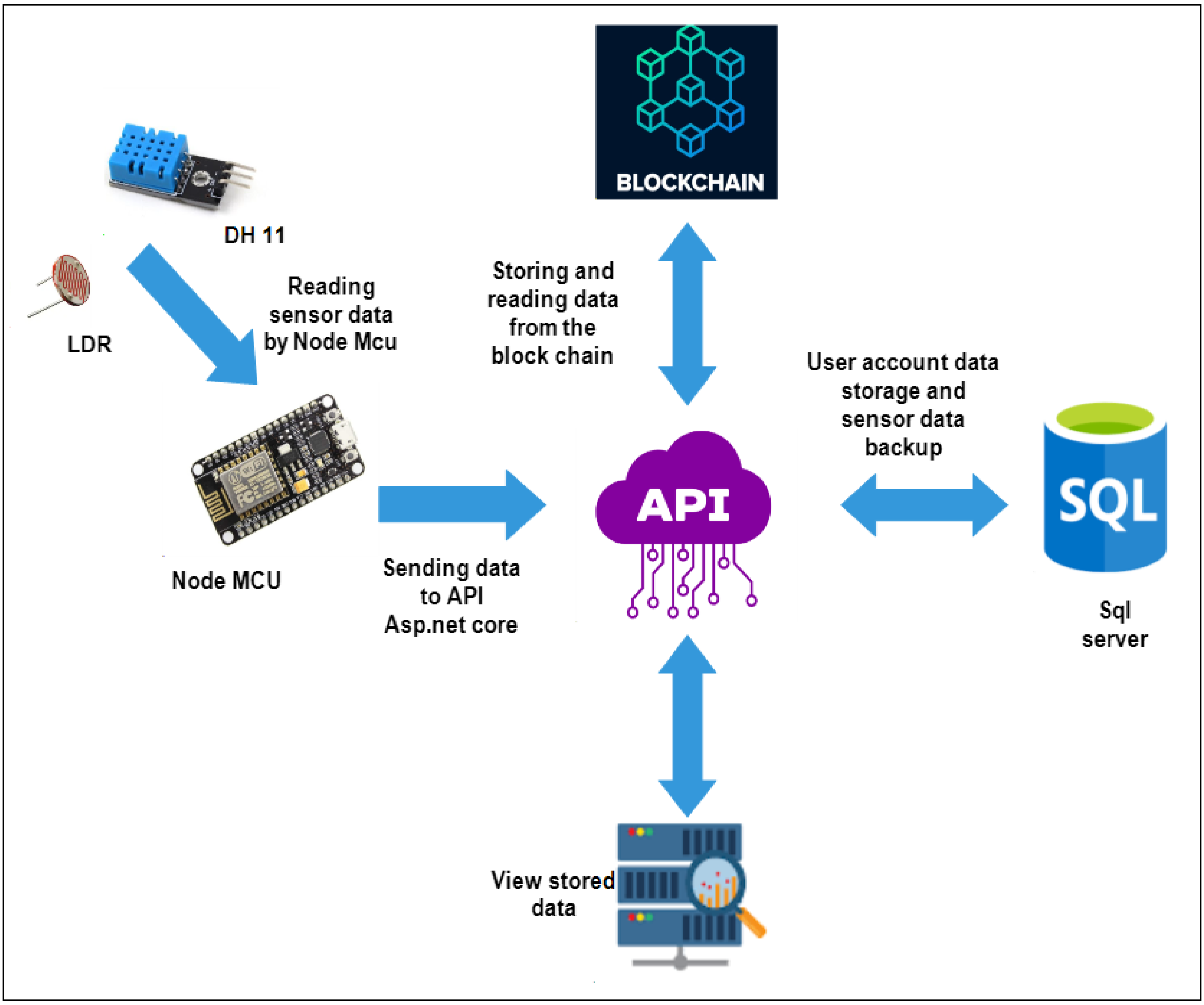

BLOCKCHAIN
DH 11
LDR
Reading sensor data by Node Mcu
Storing and reading data from the block chain
User account data storage and sensor data backup
Node MCU
Sending data to API Asp.net core
API
SQL
Sql server
View stored data

Fig 7 Method for Integrating with the Blockchain

- *Reading Sensor Data Using the Node MCU*

In this step, we program the Node MCU using the Arduino IDE to read data from the sensors connected to it. A DHT11 sensor will be connected to measure temperature and humidity. LDR sensor will be connected to measure light intensity. The sensors are connected to the Node MCU, which periodically reads the data collected from these sensors. A connection to the local WiFi network is configured to ensure internet connectivity. The collected data is sent as a JSON message to the API server using the HTTP Client library available in the Arduino IDE. The connection is also secured using Wi Fi Client Secure to ensure the integrity of data sent over the network.

- *Sending Data to the API Using ASP.NET Core*

After setting up the Node MCU, an API project is created using ASP.NET Core. A data model (Sensor Data) is created to define the structure of the sensor data to be received and stored. An API controller (Sensor Data Controller) is set up to receive sensor data sent from the Node MCU. The control module includes basic verification processes to ensure the authenticity of the received data before processing and storing it. The received data is stored in a temporary list for subsequent operations, such as saving it to the database or sending it to the blockchain. This step provides an API that receives sensor data and stores it securely.

- *Setting up a Blockchain Service for Data Storage*

We create a Blockchain Service using the Ethereum library to enable integration with the Ethereum blockchain. The service includes a function for encrypting data using the SHA-256 algorithm to ensure the integrity of the data stored on the blockchain. The smart contract is deployed to the Ethereum network using the Remix IDE, and the service is provided with the necessary data to interact with the smart contract, such as the ABI, smart contract address, account address, and private key. The service also includes a function for retrieving data from the blockchain and verifying its integrity using cryptography. The data is stored on the blockchain to ensure security and protection against tampering.

- *Displaying Data on a CSHTML Page Using Bootstrap.*

Finally, we create a new view controller (SensorDataController) and a view page (Index.cshtml) using Bootstrap to display the sensor data retrieved from the blockchain. The blockchain service is called to retrieve the stored data.

- *SQL Server Database*

The database allows the user to store data in SQL as a backup in addition to the blockchain. User data is also stored in SQL databases.

- *The Technologies used in Implementation the BCsec-DIoT Framework are as Follows:*

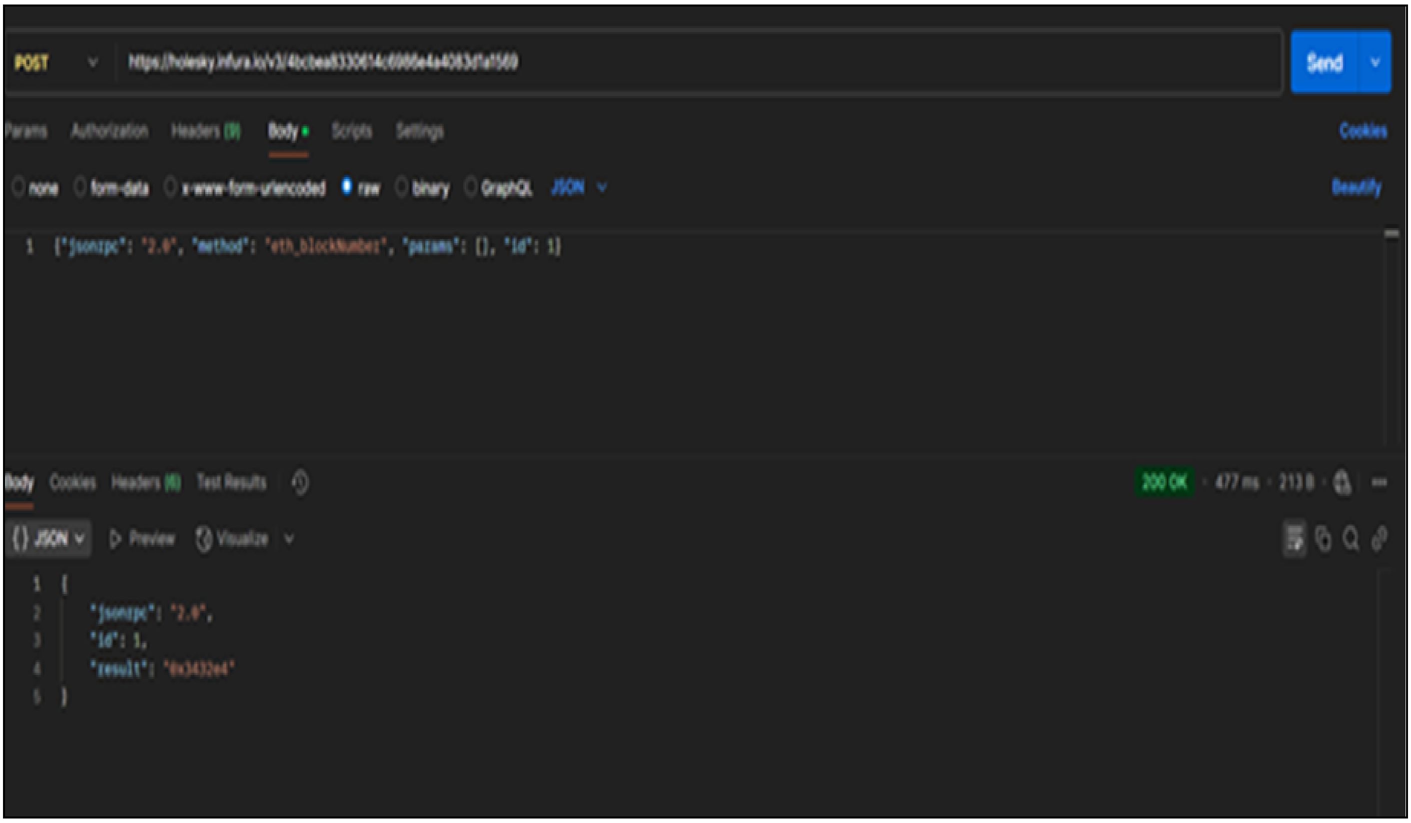
✓ *Blockchain technology:* It employed to build a security framework that improved security, reliability, access control and identity verification within IoT systems.
✓ *Smart contracts:* To control access in terms of design, development, testing, and deployment.
✓ *Ethereum networks* (Robstn or any available networks for conducting the necessary experiments).
✓ *Ethereum's own digital currency* (Ether).
✓ *Visual Studio IDEs:* An important tool for writing and executing Solidity smart contracts, a development software platform that allows communication with any Ethereum node.
✓ *Truffle:* A framework for developing smart contracts on Ethereum/a development software platform that allows communication with any Ethereum node.
✓ *Ganache:* A personal blockchain for Ethereum development/Blockchain simulator that provides development environments without real test networks or remote networks.
✓ *Front-end software:* Allows adding new users to the IoT network.
✓ *Asp.net:* A C# library for interacting with the Ethereum blockchain. Within the Ethereum network, we will use a JavaScript library that uses the JavaScript programming language.
✓ *Arduino/ESP32:* Microcontroller platforms for IoT devices.
✓ *SHA-256:* A hashing algorithm for data integrity.
✓ *Cryptography:* Cryptographic algorithms (AES) were used, keys (ECC) were used, and hashing algorithms and digital signatures (SHA-256) were used.
✓ *Remix-Ethereum Platform:* Open-source data analytics platform.
✓ Programming Languages Used

▪ Solidity: For writing smart contracts.
▪ C#: For the API server and integration with Asp.net.
▪ CSHTML: For writing web pages.
▪ C++: For programming the ESP32.
▪ C: For the Cooja emulator.
▪ JavaScript: For parsing results within the emulator.

V. RESULTS AND DISCUSSION

➢ *Smart Contract Access Test*

The test requires sending the response via the metamask server. By using post man, we get the following response which shows the contract is published and working:



https://holesky.infura.io/v3/4bcbea8330614c6986e4a4083dfaf569

```
{"jsonrpc": "2.0", "method": "eth_blockNumber", "params": [], "id": 1}
```

200 OK · 477 ms · 213 B

```
{
    "jsonrpc": "2.0",
    "id": 1,
    "result": "0x3432e4"
}
```

Fig 8 Smart Contract Access Testing Using Metamask Server / Deploy Using Post Man

➢ *Results of Adding Encryption to the Number of Packets Received*

Figure 9 shows the number of packets received by the sink node before and after encryption.

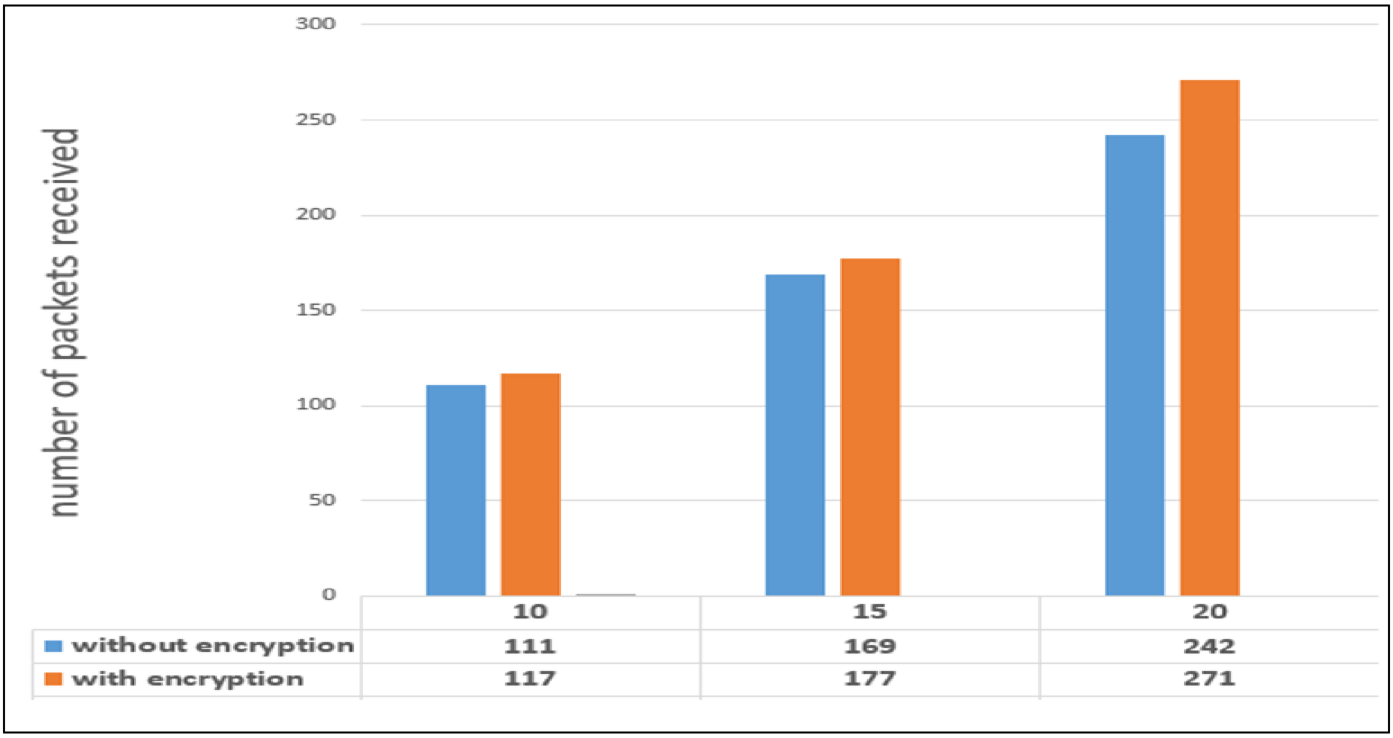


Fig 9 The Number of Packets Received

The previous results were obtained by running the simulator for 10 minutes. The results show that adding encryption did not significantly affect the size of the packets received, and therefore did not cause a significant increase or consumption of network bandwidth. The previous results also showed that the increase in the number of rice receivers reached 10.7%, which is an acceptable percentage considering the importance of securing data transmission in the manner achieved. The increase added by encryption is mainly due to key distribution and not to AES encryption, as it does not add data to the input block equal to the encryption block, but rather adds a new number of RPL messages to the packets.

➢ *Analysing the Impact of Encryption on Energy Consumption by Nodes*

Figure 10 shows the average energy consumption before and after adding encryption.

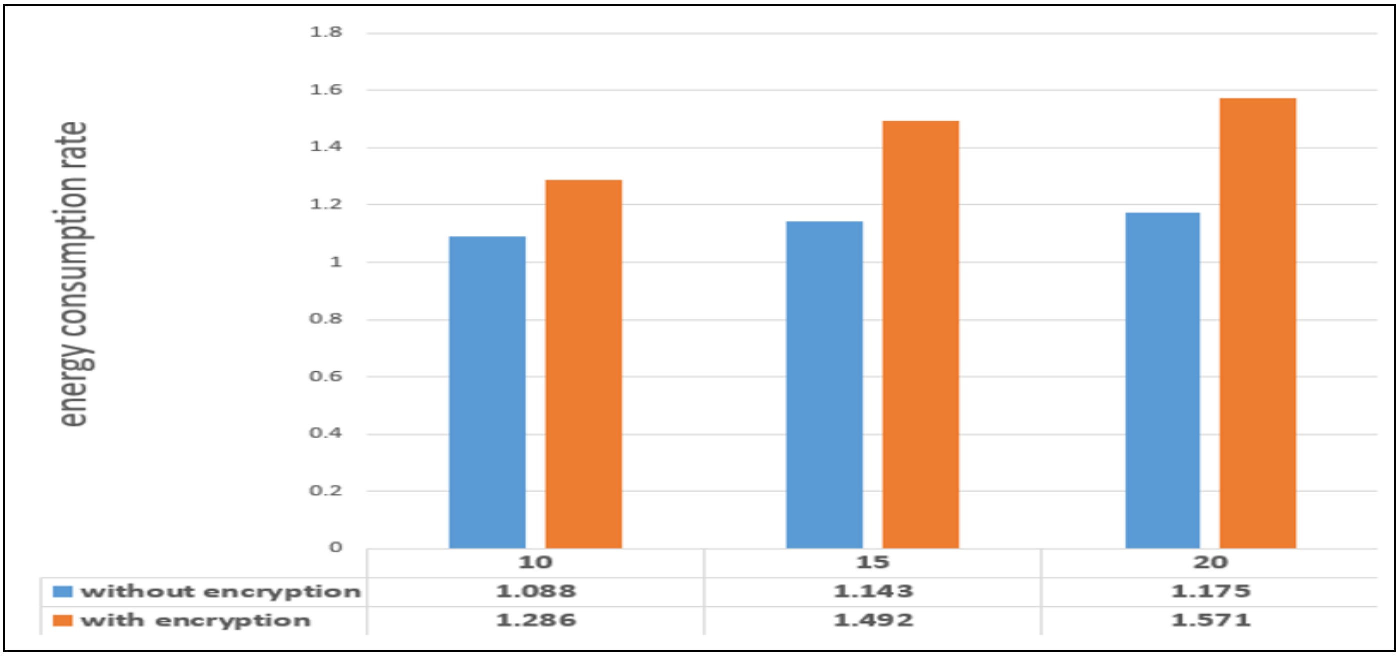


Fig 10 Average Energy Consumption Before and After Adding Encryption.

Energy consumption is one of the most important aspects of IoT networks, as sensor nodes in many applications can operate on batteries. The results showed that adding the encryption algorithm to the nodes resulted in a 25% increase in network energy consumption. Overall, at 20 nodes, this rate is considered high, but it can be covered during network implementation using larger-capacity batteries. The AES algorithm was chosen successfully due to its simple operation, but it requires more memory and therefore affects power consumption.

- *Total Time Complexity of the Encryption Algorithm*

The results were obtained using a computer with a 11th generation Gore i5 processor, 8 GB of RAM, and an SSD hard drive, as encryption speed results vary depending on the device's state.

All values are measured in milliseconds after a sink is detected for all surrounding nodes, with a maximum of 2.7 ms for the 20-node scenario.

Table 1 show the result of total time complexity of the encryption algorithm.

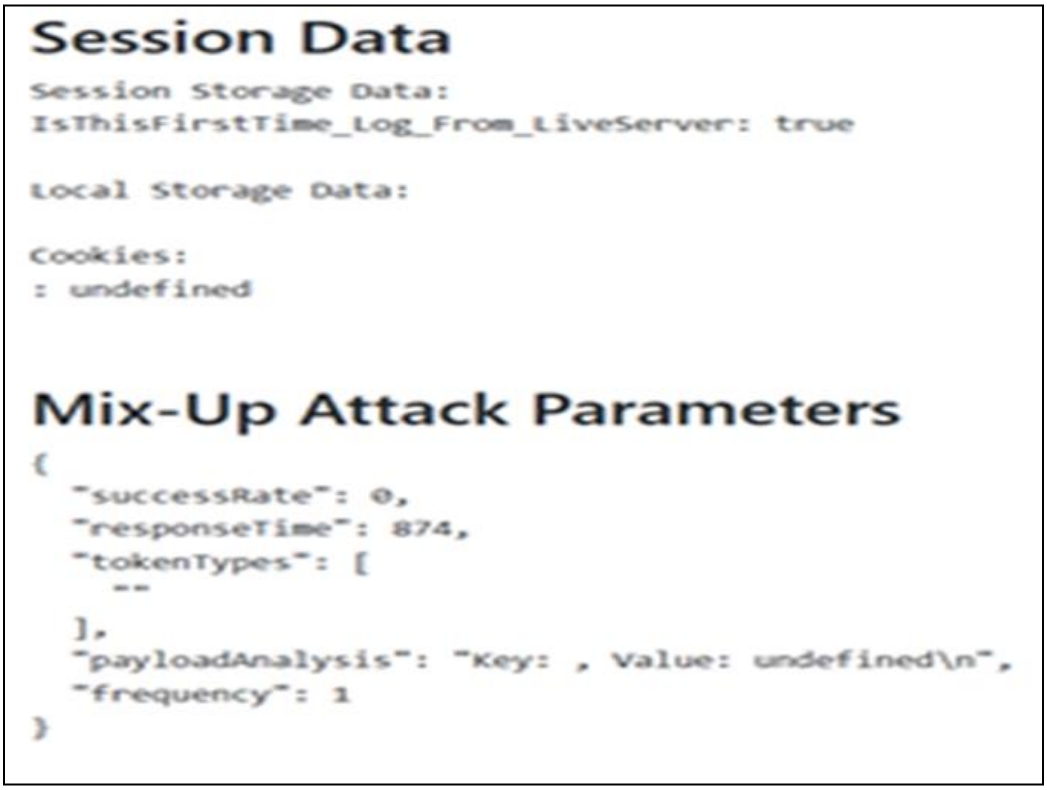
Table 1 Total Time Complexity of The Encryption Algorithm

Num of Nodes	key Distribution Time	Encoding Time Within a Node	The Decoding time Within the Sink Node
10	800	1227	1187
15	1370	1287	1201
20	1575	1301	1287

From the previous table we can found that the time delay added by the algorithm is less than a total time of 3 seconds between encryption and decryption. This is not a long time for applications that do not require significant updates, but it is a problem for real-time applications. Time delays can be addressed using IoT chips that have better processing power than the user and time can be reduced by reducing the complexity of the encryption algorithm.

- *Analysis of the Results of a Session Write Attack*

Figure 11 shows the results of a session write attack, detailing the attack results.



```
Session Data
Session Storage Data:
IsThisFirstTime_Log_From_LiveServer: true

Local Storage Data:

Cookies:
: undefined


Mix-Up Attack Parameters
{
  "successRate": 0,
  "responseTime": 874,
  "tokenTypes": [
    --
  ],
  "payloadAnalysis": "Key: , Value: undefined\n",
  "frequency": 1
}
```

Fig 11 The Results of Session Write Attack

From the previous response we showed that the attacker will be unable to access the data, and even if he does, he will obtain encrypted data that requires a great deal of effort and is almost impossible to decrypt due to the complexity of the encryption algorithms used.

- *Analyzing Blockchain Results*

To evaluate blockchain results numerically, a set of numerical parameters can be used that reflect different aspects of the system. Numerical parameters that can be used:

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25aug004

- *Response Time:*
  - ✓ Average Response Time: The average time it takes the system to process a single transaction, measured in seconds.
  - ✓ Maximum Response Time: The maximum time it takes the system to process a single transaction.

- *Transaction Throughput:*
  - ✓ Transactions Per Second (TPS): The number of transactions the system can process per second.
  - ✓ Total Transactions: The total number of transactions processed during a specific period of time.

- *Resource Consumption:*
  - ✓ CPU Usage: The percentage of CPU usage during transaction processing, measured as a percentage.
  - ✓ Memory Usage: The amount of memory consumed during transaction processing, measured in megabytes (MB).

- *Energy Consumption:*
  - ✓ Energy Consumption Per Transaction: The amount of energy consumed to process a single transaction, measured in Joules.
  - ✓ Total Energy Consumption: The total energy consumed over a specific period of time.

- *Transaction Cost:*
  - ✓ Transaction Fee: The cost associated with conducting a single transaction, measured in the currency used (e.g., Ether in the Ethereum network).

- *Data Integrity:*
  - ✓ Number of Valid Transactions: The number of transactions that were verified as valid and not rejected.
  - ✓ Number of Rejected Transactions: The number of transactions that were rejected due to lack of validation or errors.

- *Error Rate:*
  - ✓ Error Rate: The percentage of failed transactions to the total number of transactions, measured as a percentage (%).

- *Adoption Rate:*
  - ✓ Number of Active Users: The number of users actively interacting with the system over a specified period of time.
  - ✓ Growth Rate: The rate of increase in the number of users over a specified period of time, measured as a percentage (%).

Table 2 Scenario Results

Users	**1**	**3**	**5**
Average Response Time (s)	0.5	1.3	1.5
Transactions per Seconds (TPS)	20	13	10
CPU Usage (%)	30	45	50
Memory Usage (MB)	50	65	70
Energy Consumption per Transaction (Joules)	5	9	10
Transaction Fee (Ether)	0.01	0.025	0.03
Number of Valid Transactions	1000	750	700
Number of Rejected Transactions	10	25	30
Error Rate (%)	1	3	5

It is evident that increasing the number of users has a significant impact on system performance. With one user, response time is low (0.5 seconds) and system performance is high in terms of the number of transactions per second (20 TPS), with moderate resource and power consumption and a low error rate (1%). As the number of users increases to three, response time increases to 1.3 seconds and the number of transactions per second decreases to 13 TPS, resulting in increased resource and power consumption and an error rate of up to 3%. With five users, the response time drops to 1.5 seconds, the number of transactions drops to 10 TPS, and resource and energy consumption significantly increases, with the error rate rising to 4%. The results show that system performance is negatively impacted by the increase in the number of users, indicating the need to improve infrastructure and resources to achieve optimal performance.

Our results proved that integrating blockchain technology within Internet of Things systems can improving the quality of services provided, the security of data sharing within these systems. Therefore, this technology is considered to have a positive and effective impact on organizations, systems and sectors that use IoT systems, as it achieves the required service standards and enhances the protection of user records and the efficient storage and exchange of this data.

- *The Proposed Framework BCsec-DIoT Achieves the Following Security Measures/Standards:*

  - ✓ Authentication: By implementing a PKI system, a unique key pair (public/private key) was assigned to each device. The public key was stored in the blockchain, while the private key remained on the device.
  - ✓ Access Control: By restricting access to certain functions in the smart contract based on the user's role.
  - ✓ Data Integrity: By using a hashing algorithm. Using SHA-256 to hash sensitive data before sending it to the blockchain helped ensure that the data was not tampered with.

Through this research, we have demonstrated the importance of using Blockchain technology within Internet of Things (IoT) environments as an effective security technique, playing a significant and effective role in ensuring high-level

IoT cybersecurity. We have worked to improve an important aspect of security within IoT systems. Through the proposed approach, a high level of reliability has been achieved, especially when data is exchanged or stored within smart contracts on the network. Blockchain technology has been leveraged to preserve user privacy and detect any breach of these contracts, false data or any unauthorized access by attackers or unauthorized parties.

Table 3 Security Advantages Achieved by the Technologies used in Research

Technique	Security Side	Description
Blockchain	Access Control	Enforces permissions based on user roles in the smart contract.
Public Key Infrastructure (PKI)	Authentication	Public/private key pairs are used to identify devices
Digital Signature / Signing transactions	Authentication	Ensures that requests are authenticated using cryptographic signatures.
Distributed Ledger	Data integrity	Ensures that once data is written, it cannot be modified.
Hash Algorithm	Data integrity	Hashing is used to ensure that data has not been tampered with.
Public Access	Transparency	Allows anyone to verify transactions on the blockchain.
trust-free environment / No- Third Party	Decentralization	Reduces risk by eliminating single points of failure.
Smart Contract	Access Control	To control access in terms of design, development, testing and deployment.

In this research, by leveraging these technologies, an IoT system was built that achieved a strong security posture ensuring that only authorized devices can access and modify data, while maintaining the integrity and authenticity of that data throughout its lifecycle.

VI. CONCLUSION

IoT systems are inherently vulnerable to attacks from other network-connected devices such as computers and mobile phones. This necessitates a strong focus on addressing IoT security challenges and implementing countermeasures within IoT systems and their ecosystems. Blockchain technology emerges as a versatile solution, capable of functioning effectively across both lower and higher layers of communication models, providing a reliable and secure framework for developing IoT systems. protection.

This study analyzed the potential of blockchain in resolving IoT security issues, leveraging tools such as consensus algorithms, data encryption and smart contracts to create a robust mechanism for securing IoT systems over time. We proposed Blockchain Security over Decentralized IoT (BCsec-DIoT) which enhanced security and Decentralizing within IoT environments. DIoT is poised to play a pivotal role in the future of connected technologies. It promises to contribute to a safer, more scalable, and efficient IoT ecosystem. As research progresses it becomes crucial for industry leaders to recognize the potential of DIoT and integrate decentralized technologies, particularly blockchain into their IoT strategies. Transitioning from centralized IoT to decentralized systems is not merely a technological evolution but a necessary step toward a safer and more sustainable digital future.

Currently, blockchain algorithms offer the most dependable structure for securing IoT systems. Future research should prioritize enhancing blockchain's capacity, security and scalability to ensure seamless integration with IoT technologies.

The integration of Blockchain with artificial intelligence and leveraging its advanced algorithms will help address many of the gaps and obstacles within current IoT systems. This integration will provide an effective gateway to ensure the construction of smart IoT systems that are secure, fast and efficient.

REFERENCES

[1]. B. Al-Rayani, J. Al-Harbi and M. Al-Ghamdi, "Enhancing Security of IoT by Using Blockchain", Open Access Library Journal, 2022 ,Volume 9, e9148 ISSN Online: 2333-9721ISSN Print: 2333-9705.
[2]. A. D. Jurcut, P. S. Ranaweera and L. Xu, "Introduction to IoT Security", ResearchGate, 2019.
[3]. R. Hassan, F. Qamar, M. K. Hasan, A. H. M. Aman, A. S. Ahmed, "Internet of Things and Its Applications: A Comprehensive Survey". Symmetry 2020, 12, 1674. https://doi.org/10.3390/sym12101674
[4]. R. Patnaik, N. Padhy and K. S. Raju, "A Systematic Survey on IoT Security Issues, Vulnerability and Open Challenges", Springer Nature Singapore Pte Ltd, 2021.
[5]. A. Babaei and G. Schiele, "Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges", Sensors 2019, 19, 3208; doi:10.3390/s19143208.
[6]. N. Adebayo, A. O.Bajeh, M. Arowolo, E. Udochuckwu, K. Jesujana, A. Mary, A. Surajudeen and J. Onyemenam"Blockchain Technology: A Panacea for IoT Security Challenge", EAI Endorsed Transactions on Internet of Things, 09 2022 - 10 2022 | Volume 8 | Issue 3 | e3.
[7]. A. Benjaminsson, "Blockchain Applicability in IoT Systems", Master of Science in Engineering: Computer Security", May 2021.
[8]. R. Niya and S. Zurich, "Efficient Designs for Practical Blockchain-IoT Integration" Open Repository and Archive, 2022.
[9]. Sivaselvan, N., Vivekananda Bhat, K., Rajarajan, M. & Das, A. K., "A New Scalable and Secure Access Control Scheme using Blockchain Technology for IoT". IEEE, 2023 Transactions on Network and

Service Management, 20(3), pp. 2957-2974. doi: 10.1109/tnsm.2023.3246120

[10]. M. T. A. Ahmed, F. Hashim, S. J. Hashim and Azizol Abdullah, "Authentication-Chains: Blockchain-Inspired Lightweight Authentication Protocol for IoT Networks", Electronics 2023, 12, 867. https://doi.org/10.3390/electronics12040867

[11]. V. Gugueoth, S. Safavat, S. Shetty and D. A. Rawat, "review of IoT security and privacy using decentralized blockchain techniques". Computer Science Review. 2023 Nov 1; 50:100585.

[12]. A. N. Alsheavi, A. Hawbani, X. Wang, W. Othman, L. Zhao, Z. Liu and S. H. Alsamhi, "IoT Authentication Protocols: Classification, Trend and Opportunities", IEEE 2024 Transactions on Sustainable Computing, doi: 10.1109/TSUSC.2024.3492152.

[13]. JC. Priya, R. Praveen, K. Nivitha and T. Sudhakar, "Improved blockchain-based user authentication protocol with ring signature for internet of medical things", Peer-to-Peer Networking and Applications. 2024 May 13:1-20.

[14]. S. Aggarwal, N. Kumar, "Core components of blockchain". InAdvances in Computers 2021 Jan 1 (Vol. 121, pp. 193-209). Elsevier

[15]. X. Xu, C. Pautasso, L. Zhu, Q. Lu and I. Weber, "A Pattern Collection for Blockchain-based Applications", EuroPLoP '18, July 4–8, 2018, Irsee, Germany

[16]. Z. Zheng, S. Xie, N. H. Dai, W. Chen, X. Chen, J. Weng and M. Imran, "An overview on smart contracts: Challenges, advances and platforms". Future Generation Computer Systems. 2020 Apr 1; 105:475-91.

[17]. S. K. KIM && J. HUH, "A STUDY ON IMPROVEMENT OF BLOCKCHAIN APPLICATION TO OVERCOME VULNERABILITY OF IOT MULTIPLATFORM SECURITY". ENERGIES, 2019.

[18]. R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi and K. Salah, "A User Authentication Scheme of IoT Devices using Blockchain-enabled Fog Nodes", 2019.

[19]. M. Shen, H. Liu, L. Zhu, K. Xu ,H. Yu, X. Du, and M. Guizani, "Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 38, NO. 5, MAY 2020.

[20]. M. El-hajj, A. Fadlallah, M. Chamoun and A. Serhrouchni, "A Survey of Internet of Things (IoT) Authentication Schemes", Sensors 2019, 19, 1141; doi:10.3390/s19051141.

[21]. T. NANDY, M. Y. I. B. IDRIS, R. M. NOOR, M. L. M. KIAH, L. S. LUN, N. B. A. JUMA'AT, I. AHMEDY, N. A. GHANI and S. BHATTACHARYYA, "Review on Security of Internet of Things Authentication Mechanism", IEEE, 2019.

[22]. M.A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges", Future Generation Computer Systems 82 (2018) 395–411

[23]. S. Dhar, A. Khare and R. Singh, "Advanced security model for multimedia data sharing in Internet of Things", WILEY Received: 5 April 2022 Revised: 21 June 2022 Accepted: 18 July 2022 DOI: 10.1002/ett.4621

[24]. A. U. Khan, N. Javaid and M. A. K. I. Ullah, "A Blockchain Scheme for Authentication, Data Sharing and Nonrepudiation to Secure Internet of Wireless Sensor Things", 2022.