International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 15, No.1 (Jan-2024)

http://dx.doi.org/10.12785/ijcds/150129

A Survey on Leveraging Blockchain for IoT Security

Nishant Sanghani[1] **and Bhavesh Borisaniya**[2]

[1]*Gujarat Technological University, Ahmedabad, India*
[2]*Shantilal Shah Engineering College, Bhavnagar, India*

Received 2 Jun. 2023, Revised 3 Jan. 2024, Accepted 6 Jan. 2024, Published 15 Jan. 2024

Abstract: IoT is a very fast-growing technology. IoT can be defined as interconnected small smart devices linked over the Internet to communicate with each other to perform meaningful action.There are major concerns regarding the security of data being produced from millions of devices in the IoT system. Different security concerns in various IoT system tiers have been covered in this study. IoT security concerns can be reduced by using Blockchain Technology, which is a decentralized distributed ledger with several Blockchain potentials, including persistence, transparency, verifiability, encryption, and operationaly strong The paper reviews whether they make a good fit along with certain challenges of Blockchain that should be examined while integrating it with IoT for resolving various security issues.

Keywords: IoT (Internet of Things) , Blockchain, Security, Ethereum, Integration

1. Introduction

The main aim of this study is to provide an overview of Blockchain potentials that can address and reduce various security concerns present in the IoT system. In this paper, different use cases in IoT like firmware updates, Device management and monitoring, PKI infrastructure for IoT, different frameworks and architectures for integration with IoT using Blockchain has been examined concerning the IoT system's security features.

The number of physical devices being connected to the internet is increasing quickly. According to [1], there will be 8.4 billion connected devices worldwide in 2020 and a projected increase to 20.4 billion by 2022 [1]. By 2022, this figure is projected to increase to 20.4 billion. IoT applications are being used more often all around the world. Western Europe, North America, and China are the primary regions driving this. Machine-to-machine (M2M) connections will increase from 5.6 billion in 2016 to 27 billion in 2024. According to the rise in numbers alone, IoT is one of the main rising markets that could act as a foundation of the expanding digital economy. According to [2], the IoT market is predicted to expand in terms of revenue from $892 billion in 2018 to $4 trillion by 2025. Due to lot of data created from numerous IoT devices in the IoT Ecosystem, there are security and privacy risks with this wide range of IoT applications. IoT security is primarily concerned with dangers or challenges related to privacy, authentication, confidentiality, integrity, accessibility, single point of failure, and other areas. IoT systems are vulnerable to a variety of cyber threats as a result of all these problems. Deployed IoT applications have been impacted by noteworthy security and privacy breaches on a global scale. According to estimates from [3], infecting over 2.5 million devices linked to the Internet, the Mirai attack in the year 2016 started a distributed denial of service (DDoS) campaign.IoT devices' low security and inexpensive electricity make them a doorway for adversaries to enter household and commercial networks, giving them simple access to user data. The Internet of Goods is expanding beyond only physical goods and objects. The successful implantation of IoT devices into human bodies to track the health of various organs has been attempted on several occasions, according to [4]. Attackers may target such devices to manipulate data or trace down a specific person's whereabouts. There are several layers in any IoT system, but with security concerns in mind, there are four key layers. The perceptual layer is the top layer, and it is responsible for physically using sensor devices to sense data from the environment around us. The network layer receives the sensed or gathered data before processing it further and taking action that is useful across many cloud services with remote or local storage. With the use of numerous APIs and middleware technologies, the third layer, known as the support layer, serves as a bridge between the network and application layers to facilitate easy communication between them. The application layer, which deals with users' needs to access various services using IoT devices, is the final layer.

Blockchain is a secure, distributed, unchangeable, and open source ledger that records different transactions on a peer-to-peer network. Blockchain transaction is shared on the public ledger and is actively verified and validated by the

E-mail address: nssanghani15@gmail.com, borisaniyabhavesh@gmail.com

majority of miner nodes. In Bitcoin , miners audit a block by calculating a hash using the first few digits of the value set as the target difficulty. Block data cannot be deleted or changed once transactions have been validated and verified by consensus. The various security risks that Blockchain can address include those related to non-repudiation, confidentiality, availability, integrity and access control of IoT systems.

Paper structure is as follows. In Section II we examine the concept of IoT with its architecture composed of different layers. In Subsection B of Section II, Security requirements in IoT have been discussed with its layered architecture. Layer wise security issues in IoT systems have been listed out according to security architecture. In Section III we introduce Blockchain with its block structure and defining different terminologies with various potentials of Blockchain which can help to mitigate various security issues or threats in IoT systems providing several solutions for the same. Some challenges of Blockchain in incorporating with IoT systems for security issues have also been drafted. Finally, in Section IV & V we inscribe open issues and research gaps or challenges in integrating Blockchain Technology for mitigating various IoT security issues for research scholars and furnishing our conclusion in Section VI.

2. Internet of Things (IoT)

IoT can be defined in simple terms as a network of manmade objects or devices capable of transferring data through the Internet and acting intelligently. The Internet of Things (IoT) also refers to the meaningful action that is triggered subsequently after an exchange of analyzed data. For example, smartwatches give alerts on notifications received from smartphones, smart bands keep measuring heartbeats, Sensor to measure temperature etc. IoT applications examples are Smart home, Health Care, Smart Cities, Wearables, Industrial Automation, Energy Management (Smart meter) etc.

The IoT includes all the things from the body sensor to the components of cloud computing. It is also interconnected with major types of networks such as distributed, grid, ubiquitous etc. IoT has been covering all over the world of IT from manual analysis action to automatic decision-making action or things without human intervention, for example, adjusting air conditioner temperature according to our body/room temperature, remotely controlling electrical appliances, remotely accessing CCTV footage etc. Sensors are core components for generating as well as collecting data, which can lead to certain meaningful actions being performed. The data collected from different types of sensors for particular actions are private information and need to be secured.

Vast growth of IoT devices makes them appealing targets of various cyber-attacks. IoT devices become more vulnerable to threats as they generate massive data with specific constraints which can lead to processing overhead and also a single point of failure in the case of centralized architecture. Also, Wireless Sensor Networks (WSNs), Cyber-Physical Systems (CPS) or Machine-to-Machine (M2M) are evolved as integral parts of IoT. Hence, security issues in WSNs, CPS or M2M continue to grow in context with IoT. Entire IoT architecture with different layers must be secured from various types of vulnerabilities or attacks which may obstruct different services provided by IoT as well as may threaten the privacy, confidentiality and integrity of data. In recent years, there have been enormous efforts to manage security issues in IoT.

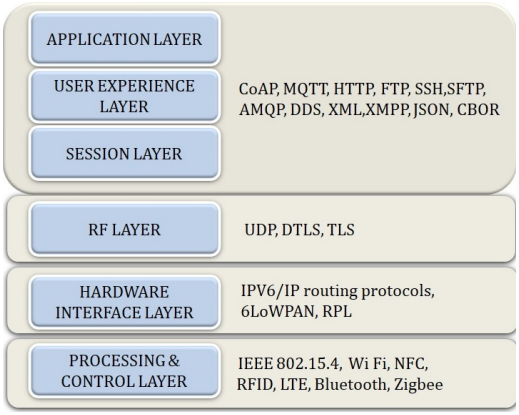

Figure 1. IoT Architecture

A. IoT Architecture

IoT has an architecture clearly defined in the form of different layers. The Open System Interconnection (OSI) model specifies networking architecture to implement protocols in seven layers from Layer 1 as the physical layer to Layer 7 as the application layer. Each layer has clearly defined protocols with proper hardware/software working from that succeeding layer [1]. The same is the scenario with IoT. Seven Layers have been identified in IoT Architecture as shown in Figure 1

Application Layer

It deals with different applications, which are built as well as operate with the support of the rest of the layers. The applications can vary in the range from simple automation to smart city. Other examples of applications are smart meters, smart homes, smart parking, smart retail, smart agriculture, etc.

User Experience Layer

This layer is fully concerned with the end user experience especially rich UI (User Interface) features and design which provides the best experience while using the different services/ systems or products. Object oriented programming languages, scripting languages, and other different analytical tools, etc.

Session/Message Layer

Session management is more important in IoT as it is general networking that is being directed by the OSI layer. Some protocols such as CoAP, MQTT, HTTP, FTP, SSH, and SFTP are used to oversee how messages (data) are broadcasted to the cloud server or gateway server.

RF Layer

The RF layer plays an important role in the communication channel (short or long range). Protocols that can be used for communication as well as for the transport of data based on RF are Wi-Fi, NFC, RFID, LTE, Bluetooth, etc.

Hardware Interface Layer

This layer majorly concerns about the flawless communication between all things in IoT. Different components and communication standards like CAN, RS232, Serial/ Parallel Standards, SPI, SCI, FC, etc. occupy this layer.

Processing and Control Action Layer

This layer contains core components for IoT. Microcontrollers or processors are present in this layer. Different development kits are available in the market such as Arduino, NodeMCU, PIC, and ARM development boards to do processing of data collected from the sensor layer and determine whether the data is meaningful or not.

Physical or Sensor Layer

This layer is composed of hardware or physical components which includes different sensors. Different sensors like temperature sensors, pressure sensors, humidity sensors, etc. as well as other components like industrial automation, PLC, actuator, etc. are used to collect data by sensing.

B. Security in IoT

In any digital technology, a prime concern is the security of data or information and IoT is no exception. A Big challenge here is security and privacy of data being generated and processed for meaningful action over the Internet with the help of mobile or broadband networks, Bluetooth sensor networks and so on.

There are different IoT security aspects or perspectives, which are being briefed in further discussion. Microcontroller unit in the IoT system has firmware that can be used to enhance services and overcome security threats by updating them [2]. More secure channels can be used for pairing stages of IoT devices by limiting access and use of public networks. An appropriate and secure protocol should be used for binding user and IoT devices. User authentication is required whenever the controller wants to link the port in a private or local network or needs to give commands to control things in an IoT network. Sometimes cloud services are used or required for authentication, whenever the controller is on a public network in an IoT system. Abnormal behavior can be notified to the users as well as big data analytics can be processed in the cloud on specific data that is being collected through the different devices in the IoT system over the cloud. The basic IoT security and privacy aspects are data, software, hardware, OS/firmware and networking.

1) Security Architecture of IoT

It is shown in Table I. The main four layers deal with various applications and security threats which are being defined and discussed in detail as followed in a further section.

Perceptual layer or sensor layer is the most basic layer which will just collect the data or information like properties of things or objects, environmental conditions etc. from the different IoT devices using the sensor or physical equipment like RFID reader, GPS or all kinds of sensors, etc.

Network layer is responsible for broadcasting and communicating different information and data over the different channels in the different networks like mobile communication network, wireless network, satellite network, etc. as well as handling the data that is being collected through the different sensors from the previous layer.

Support layer will construct a dependable platform for the application layer. Data processing, data mining, feedback and intelligent handling are being done for meaningful actions to be performed. It acts as a bridge between the application layer and the network layer.

Application layer provides personalized services as per the user's requirements and needs. It helps to access the different IoT devices through different interfaces like computer systems, mobile phones, televisions and other such smart devices.

2) IoT Security Requirements

For secure implementation of IoT systems different parameters as well as mechanisms has to be taken into consideration across different layers as shown below:

Perceptual Layer

Any illegal access can be prevented using authentication, which is very essential. Data confidentiality should also be taken care of during the transmission between different devices or nodes. Different cryptographic techniques can also be used for securing the data which may lead to more resource consumption. Lightweight encryption techniques having cryptographic protocol and algorithms help to resolve this issue.

Network Layer

Access control as well as the availability of the different services and data over the various types of networks should be a major consideration. Data integrity and confidentiality have to be established on a priority basis as it has to be transmitted over the network. Distributed denial of service attack in the network is a serious focus in the IoT domain.

TABLE I. IoT Security Architecture

Layer Name	Various Applications	Security Threats
Application Layer	Smart Home, Smart meter, Smart healthcare, Smart transportation, Smart buildings, Smart grid security, Environmental monitoring security	Data Breaches, Illegal Interruption Attacks, HTTP Flood Attack, Malware Code Injection Attacks, Repudiation Attack,Sniffing Attacks, SQL Injection Attack,Access Control Attacks
Support Layer	API, Web services Data center, Cloud	SQL Injection Attack, MITM (Man-in-the-Middle Attack), Signature encasing Attack, Flood Attack, Cloud Malware Injection
Network Layer	Transmission, GPRS, Internet, Wi-Fi, Routing	Routing low power & lossy network routing attack, Sybil attacks, duplication, attack, Phishing Site Attack, Routing Attacks, Data Transit Attacks, Insecure neighbor discovery,Access Attack,DDoS/DoS Attack
Perceptual or Sensor Layer	RFID, WSN security, Temperature sensor, Actuator, ultrasonic sensor, smart smoke detection sensor and others	Insecure initialization, Malware Code Injection Attack,Jamming adversaries, False Data Injection Attack,Eavesdropping and Interference, Booting Attacks, Capture Node, Sleep Deprivation Attacks,Side-Channel Attacks

Support Layer

Cloud as well as Edge Computing falls in this layer for multi-platform computation of data. Different cryptographic techniques are being used to secure the data. Availability as well as single point of failure should be considered in this layer.

Application Layer

It provides different services to the end users in an IoT system as per requirements. Specific issues in this layer such as data confidentiality, data integrity, data breaches and data privacy issues are there. Security concerns in this layer vary according to the distinct applications being used.

C. Security Challenges in IoT

Each one of these layers in IoT is dealing with various technologies that lead to a number of security issues and threats as shown in Figure 2. Here various security issues and threats are focused on different layers of IoT architecture that are discussed as follows:

1) Perceptual or Sensor layer security issues

Physical actuators are mostly the responsibility of the perceptual layer. Sensors capture the movement of the surrounding when they are fitted. [5]–[7]. Actuators carry outs meaningful actions on the physical system according to the data sensed by the sensor. Major security issues or threats that can affect the perceptual layer are as follows:

Capture Node: IoT applications contain a lot of low power nodes like sensors and actuators, are included in IoT systems and applications. In this attack adversaries replace original node to malicious node which compromises security of IoT systems [8].

Malware Code Injection Attack: During the process of remote firmware update malicious code is inserted by an attacker in the memory of IoT devices. With the help of such malicious code attacker may try to control the IoT system and can lead to perform some malicious or unintended activity.

False Data Injection Attack: In this attack incorrect or false data is inserted in the IoT system which may create false data with malfunctioning of the IoT application. This method can result into DDoS attack.

Side-Channel Attacks: This kind of assault is brought on by excessive power utilization, attacks based on laser, timing, or electromagnetic, all of which have the potential to expose sensitive personal information.

Eavesdropping and Interference: According to [9], IoT applications frequently comprise of numerous nodes placed in open spaces. During the data being transmitted or authenticated, attackers may eavesdrop and intercept it.

Sleep Deprivation Attacks: By deploying malicious code to perform endless loops or by boosting the power consumption of edge devices leading to battery drainage. A Denial of Services attack on the IoT system may result from this.

Booting Attacks: Because the booting process's built-in security is not activated, IoT devices are susceptible to a variety of assaults. Considering this as an advantage, attacker can restart the node.

Jamming Adversaries: This kind of attack targets network failure by sending out jamming signals utilizing various frequency signals without adhering to a predefined protocol [10], [11]. The Node failure in the IoT system has a significant influence on the network

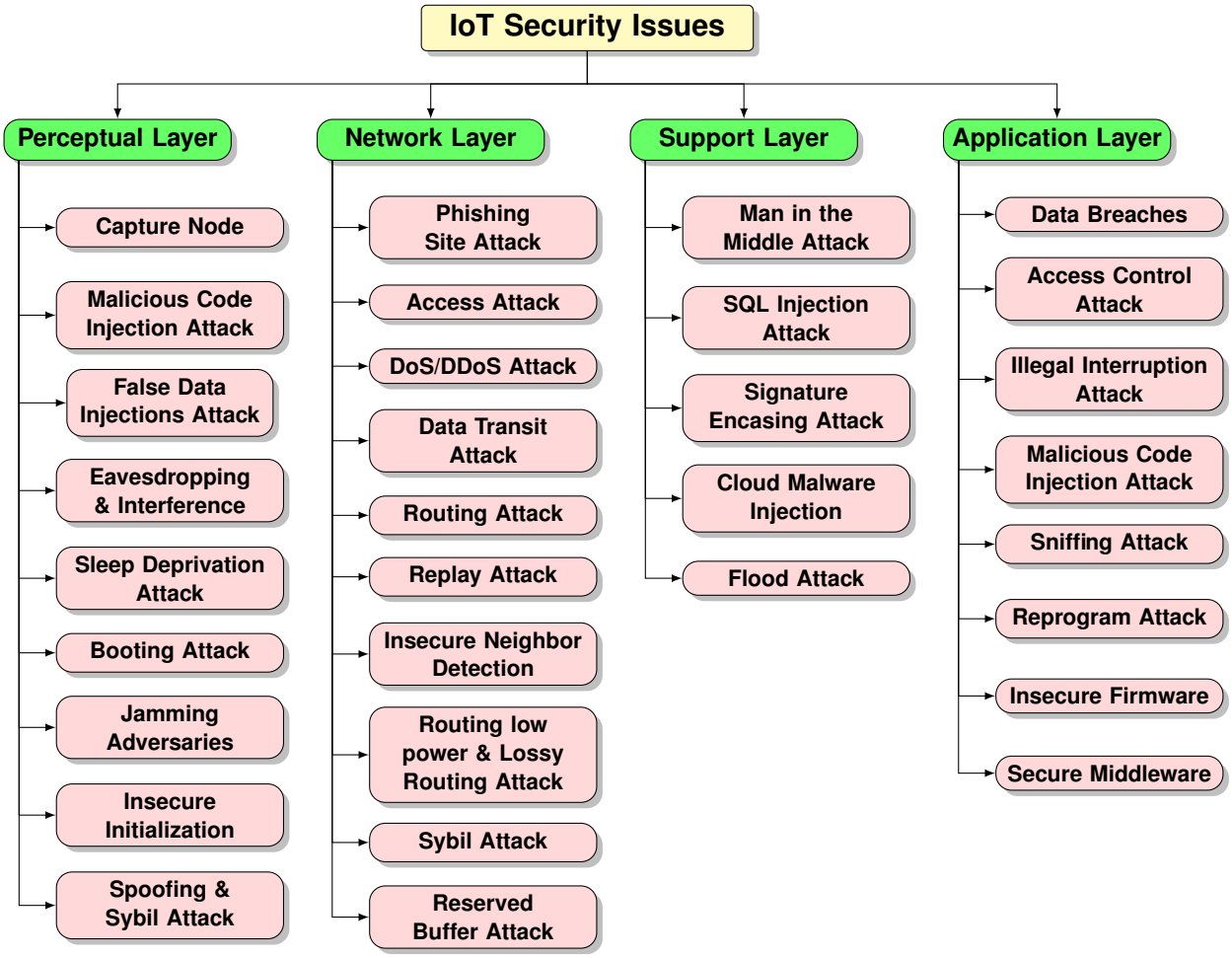

Figure 2. IoT Security Issues

as well as on the transmission of data by various authorized nodes.

Insecure Initialization: The initialization of devices at the physical layer demonstrates proper system behavior and operation. [12], [13], it is necessary to implement a safe system for the same without infringing user privacy or interfering with network functions. To work better, unauthorized access at the perceptual layer must be stopped.

Spoofing and Sybil attacks: Such an attack is the work of malicious Sybil nodes. To exhaust network resources, they exploit false identities while disguising random forgeries of MAC values from various devices [14], [15]. This could prevent the genuine nodes from getting access to resources.

2) Network layer security threats:

The data collected from the sensing layer is sent for processing to the computing. The major security issues are as follows:

Phishing Attack: Every time a user accesses a website on the internet, an attack of this kind takes place. When user credentials are stolen, the entire Internet of Things system becomes open to numerous cyber attacks. According to [16], the network layer is extremely susceptible to these attacks.

Advanced persistent threat Attack: it is the same as access assault. Here attacker gains unauthorized access and can steal vital data rather than harming the network. Due to constant transmission of vital data between applications of IoT, it makes them extremely susceptible to such assaults [17].

DDoS/DoS Attack: It involves the attacker bombarding intended servers with a high volume of unsolicited requests. As a result, the target servers are unable to offer different services to actual users. With the use of several sources, attacker overwhelms the target server is called as a distributed denial of service. By sending repeated requests to the incorrectly configured devices of IoT, the Mirai botnet assault took use of

this vulnerability and blocked a many services [18].

Data Transit Attacks: Data processing and data storage are both included in IoT systems. Important data is more susceptible to cyber attacks when it is in transit or stored locally and in the cloud. Since, a lot of data movement between sensors, actuators, the cloud, etc. in applications of IoT, data breaches are more likely to occur.

Routing Attacks: In an IoT system, compromised nodes may attempt to change the routing pathways during the transmission of data in the network in this attack. A specific type of routing attack known as a sinkhole invites nodes to routing traffic via it by advertising a fictitious shortest path [19], [20]. Another assault that, when coupled with others like sinkhole attacks, might cause a serious security. A warm hole is a remote link between two nodes that allows for quick packet transfers. An warm hole can be established between a compromised node and a internet-connected device by an attacker [21]–[23].

Duplication attacks: IPv6 packets must be fragmented by devices that conform to the IEEE 802.15.4 standard, which is characterized by a small frame size. Re configuring the fragment fields of packets could lead to resource depletion, buffer overloads and device reboots in layer 6LoWPAN, according to [24]. According to [25], malicious nodes transmits matched fragments obstruct packet rebuilding and the process of other packets gets declined.

Insecure neighbor Detection: in IoT architecture, each device consists of a unique network identifier. The transmission of identification messages must be safe to ensure that the information transmitted to a device in an end to end connection is received at its intended destination. The neighbor discovery phase is a series of tasks, e.g. finding the router and resolving the address before data transmission [26]. If the neighbor discovery packets do not have adequate verification, their use may lead to serious consequences such as denial of service.

Reserved Buffer attack: This can be exploited by an attacker by delivering incomplete packets because the receiving node needs to set up buffer space to reassemble the incoming packets [25]. Since the space is not available can lead to denial-of-service by dropping the fragment packets.

Routing Low power & Lossy Network attack : The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is susceptible to several assaults that are launched by infected network nodes [27]. The attack might cause resource exhaustion and eavesdropping.

Sybil attacks: Sybil nodes in the network communicate using the false identities to do damage like conducting phishing attacks, spreading malware, or sending spam [28], [29]. This node can be used to degrade network performance and breach data privacy.

3) Support layer security threats

The support layer's function in the Internet of Things is to serve as a link between the network layer and the application layer. Bandyopadhyay.et.al [30] mentions that the support layer can also provide strong processing and storage Potential. This layer offers API interfaces to meet the needs of the application layer. A stable and resilient IoT application needs a support layer, but this layer is also vulnerable to numerous assaults. This assaults can seize the whole IoT Programme by compromising middleware. Other important security challenges in the support layer are database security and cloud security.

The application layer and the network layer are connected by the support layer in IoT to become a bridge between. The support layer can also offers storage and strong computing. The application layer API interfaces are provided by this layer. The support layer plays an essential role in providing an efficient and reliable IoT application, but it is also vulnerable to different attacks. By infecting the middleware, these attacks can control the entire Internet of Things application. Another major security problem in the support layer is cloud security and data protection. Various threats in the support layer are as follows:

MITM (Man-in-the-Middle Attack) : The MQTT broker, which essentially serves as a proxy, facilitates communication between clients and subscribers utilizing the publish-subscribe mechanism. Using a MQTT broker,the publisher and subscriber can be kept apart from one another and communicate without even knowing the destination. If the attacker takes over the broker and acts as a man in the middle, he can completely control all communications without the client's knowledge.

SQL Injection Attack : Additionally vulnerable to SQL Injection (SQLi) attacks is middleware. Attackers can insert dangerous SQL statements into a program using this technique [31], [32]. Then he can then gain control to fetch any user's private data and even modify information in the database [33] as an example. OWASP's Open Web Applications Security Project describes SQLi as one of the serious threats to web security in its top 10 2018 paper. [34].

Signature Encasing Attack : Different XML signatures are utilized in web services [35]. The attacker is capable of executing commands or modifying intercepted messages through a signature encasing attack, which breaks the encryption algorithm [36].

Cloud Malware Injection : The attacker has three options in this attack: take over, inject infectious code, or introduce a virtual machine into the cloud. The attacker will pretend to be a legitimate service when attempting to create an instance of the virtual machine or malicious services module. In this way, a hacker could gain access to a victim's requests for service by collecting information that can be adjusted according to the situation.

Flood Attack : This attack degrades the functions and quality of service (QoS) nearly identically to a DoS attack in the cloud. Attackers continue to request a service multiple times so that they can increase the demand for cloud servers to drain their resources.

4) Application Layer security threats:

End consumers receive services directly from the application layer. The layers contain applications based on the Internet of Things, like Intelligent Households, Smart Cities, and Smart Grids. There are two specific security vulnerabilities exclusively at this level, and none in the rest of the hierarchy: data theft and privacy concerns. The security issues for this layer differ from one application to another. The major security problems that need to be dealt with by the application layer are covered in this discussion.

Data Breaches: A lot of sensitive data is involved in applications for the Internet of Things. The applications of the Internet of Things is loaded with big amounts of data, which makes them much more vulnerable to attack than at rest. Users will be reluctant to register their data on Internet of Things applications when they are exposed to the risk of a data theft attack. Encryption, data isolation, user authentication, privacy management, and so on are some of the strategies and protocols used to protect Internet of Things applications from data theft.

Access Control Attacks: Access to data and accounts will only be authorized using a system known as access control, for authorized individuals or processes. IoT applications are particularly vulnerable to access control threats once that access has been compromised.

Illegal Interruption Attacks: In extant literature, these attacks are sometimes known as service interruption attacks. These attacks have occurred on a many occasions in the Internet of Things applications. These attacks have prevented lawful users from accessing the services of IoT applications because they create a network or server whose congestion is artificial.

Malicious Code Injection Attacks: If the system is exposed to malicious scripts and misdirection as a result of poor code checks, this may be the first access point chosen by hackers. Attackers usually inject malicious script using XSS Cross Site scripting into a reputable Web site. If a XSS attack is successfully performed, the IoT account can be compromised and the Internet of Things systems may fail to function.

Sniffing Attacks: Attackers will be able to monitor network traffic from the Internet of Things applications via the sniffer application. If the attacker can access personal user data because of an insufficient security measure, it may not be prevented. [37].

Reprogram Attacks: If the programming process is not secured, attackers could try remotely reprogramming Internet of Things devices. This could result in the IoT network being hijacked [38].

Insecure firmware: Various IoT vulnerabilities, such as those brought on by unsafe software or firmware, are listed in [39]. Carefully testing the code that uses languages like XML, JSON, XSS, and SQLi are necessary. Similar to this, it's important to update software and firmware securely.

Secure Middleware: To deliver services between the different players of the Internet of Things paradigm, our Internet of Things middleware must have sufficient security. Several Middleware interfaces and environments must be used to provide safe communication [40], [41].

3. Blockchain

Blockchain was presented in 2008 and executed in 2009 also called a Distributed Ledger (Nakamoto, 2008) [42]. Blockchain technology is a secure technique for authenticating, verifying, and authorizing data generated as well as a storage system providing decentralized big registers [43]. Four main ideas form the foundation of Blockchain technology: A peer-to-peer network (i) gets rid of the central Trusted Third Party, suggesting that each node in the network has equal access rights. A set of private and public keys may be used to communicate among the nodes in this network. The public key is the address for the network, and transactions are signed using a personal key. (ii) Open and distributed ledger: This ledger functions as a book of accounts, compiling all network transactions in reverse chronological order. The fact that each node has a copy of this data structure means that it is not a centralized entity. The ledger is available to everyone and is public. The location of the asset and the amount that each user has in their account are both visible to everyone on the network.

In addition, every node on the network is capable of determining if a transaction is genuine or not. (iii) In situations like this, in which each node contains its own copy of a single logbook, it is essential that the log files be synchronized between nodes. To achieve that objective, three main steps must be taken: (a) broadcasting new transactions to the network on an open basis; (b) verifying them, and (c) adding those validated transactions to the ledger. (iv) Mining: After a block has been validated, a

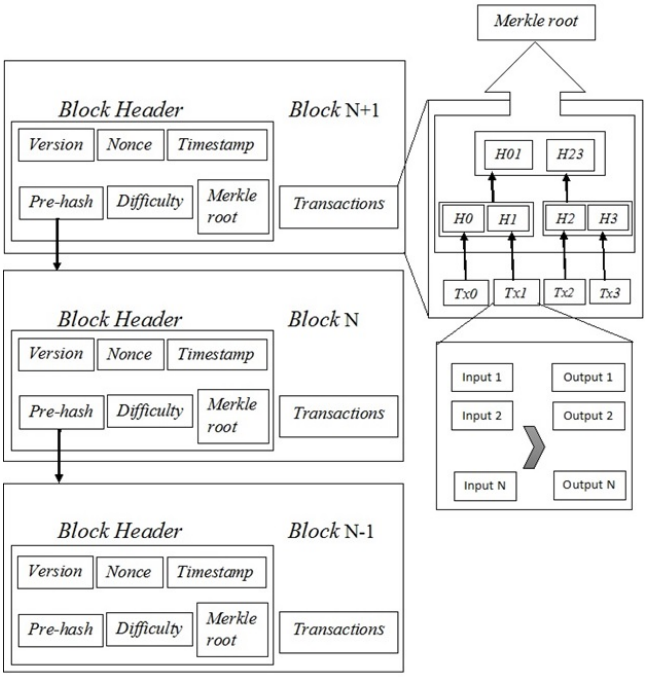

Figure 3. Blockchain Structure

miner will append transaction information to it. Blocks are safeguarded by Blockchain miners and joined together to build chains in the ledgers.

As defined in Figure 3, The Merkle root, the hash of all transactions that are held in a block, header, preceding block's hash, and additional transactions are part of each block. A transaction between network members that is organized into blocks is how the Blockchain process is defined. Cryptographic methods that rely on the rules, also known as the consensus process, are used to validate the block and save it on the network by a child. This method is known as "proof-of-work" (POW) in the Blockchain for Bitcoin and "proof-of-stake" (POS) in the Blockchain for Ethereum. If the block is accepted, it is time-stamped, added to the Blockchain, and then validated. Following that, the receiver and the entire network can see the transaction [43].

The first block called "genesis", in the chain and has no parents and is shared by all clients in a Blockchain network, is an exception to this rule. A chain of blocks, or the Blockchain, shall be formed by building a connection between them. To determine the current Network wide Status for Data Exchange, any node that has access to this Ordered List of Blocks can read it.

A. Blockchain Potentials

Different Blockchain characteristics can be leveraged for solutions to privacy and security issues of IoT, as follows [43]:

1) Basic Security Requirements

Integrity can be defined as no tampering with data is done without permission. Blockchain provides cryptographic mechanisms to ensure integrity.

Availability can be defined as data available as per need. Blockchain ensures this by making various copies distributed over the network.

Privacy can be defined as authorized access is granted. Blockchain provides this by anonymization by hiding user identities.

Authentication can be defined as certifying the user to access. Private keys are used for this purpose in Blockchain.

Non repudiation can be defined as no user can deny the information sent or received. History of all transactions are stored in Blockchain to support this feature.

2) Shared / Distributed ledger

It is a feature where all processed transactions or data are stored in a decentralized way with a copy to every node in the network. This leads to a solution for a single point of failure and all participants have equal rights.

3) Smart Contracts

They are automated programs that execute when certain conditions are met. This helps reduce audit costs, execution, arbitration, and fraud.

4) Trust

Without the aid of third parties, Blockchain fosters trust among previously untrustworthy parties. Users are no longer obliged to have confidence in centralized organizations to manage their data streams. As a result, harmful third-party organizations are unable to gather consumers' personal information.

5) Immutability

The record of transactions is processed or calculated by cryptographic hash and stored in the block. Due to such process, such records will be permanently immutable as it is verified and validated by different miner nodes. As each block is logically linked to each other in the Blockchain, change in any block requires a change in all subsequent blocks which is practically not possible.

6) Anonymity

When any transaction occurs then the address and transaction details are recorded in encrypted hash form by the miner node in the Blockchain. Hence, there is no link between transactions and user identity.

7) Consensus

It is a reliable basic trust mechanism. It denotes a widespread understanding of a group's existence. It enables you to decide for yourself without consulting a third party or reliable authority. Examples are PoW PBFT, and PoS (Proof of Stake).

B. IoT Security Solutions through Blockchain

Blockchain Technology, which is aimed at a major role in managing, controlling, and most importantly protecting IoT devices have been identified as important attention seeking technology by industry and the scientific community. This section explains the key role of Blockchain as a crucial technology that could allow us to offer an effective solution for today's complicated security concerns with IoT. This Section will review regarding different security threats of IoT with its different possible solutions through various intrinsic Blockchain features that can be helpful to IoT and particularly security of IoT.

The use of Blockchain in IoT applications has various benefits. Table II provides a summary of some specific IoT security concerns and suggests various Blockchain-based potential solutions. IoT applications confront several security challenges, which were already covered in Section II. In this section, we will discuss the key advantages of using Blockchain Technology in Internet of Things applications.

The Table II summarizes the specific security problems in the Internet of Things, as well as potential solutions through Blockchain. In Section II, it has already covered different security issues for applications connected with the Internet of Things. Below is a summary of the main advantages to be gained from including Blockchain in Internet of Things applications.

Blockchain stores data processed by IoT devices: Applications for the Internet of Things (IoT) use a wide range of interconnected devices. Other gadgets are connected to and in control of these devices as well. This setup also provides additional cloud connections that make it possible to use Internet of Things applications from anywhere. Because of this large amount of data storage space, it is possible to store and protect against its abuse via the use of Blockchain. No matter what layer of an Internet of Things application is used, Blockchain can be the right solution to store and transport data.

Blockchain's distributed architecture enables secure data storage: In view of the decentralized nature of a Blockchain, it can minimize the possibility that there'll be a single failure point which is an issue for numerous cloud borne IoT applications. The storage of data produced by devices on the Blockchain is easy and safe, even if they are miles apart [55].

Encrypting data with a hash key that is validated by miners: In Blockchain, the 256-bit hash key for the data can be kept. The hash key is associated with the original data, and the actual data will be kept in the cloud. The data's hash will change if the data changes in any way. The information is now private and protected. The size of the data would not effect on the size of the Blockchain because each hash value is stored in a chain. The data can be accessed from the cloud using a hash of the data, which is used to identify interested parties and those who have been authorized to access that data. The use of Blockchain as a solution would reduce the risk that devices will store incorrect information since every set of data is adequately verified by different miners of the BC network.

Protection against spoofing and data loss attacks: To fake attacks against IoT applications, a new adversary node has joined the network and is now behaving as if it belongs to the original network. In the use of a spoofing attack, an adversary may be able to quickly fetch, observe or inject data into the network. In the face of such threats, Blockchain is an effective defense. On the Blockchain, each valid user or device is registered, and devices can quickly authenticate and identify one another without the use of certification bodies or central brokers (Dickson, 2016).IoT devices carry a risk of data loss due to their low power nature. There may be situations where both the sender and the recipient lose the data as a result of certain external environmental problems. Utilizing Blockchain can prevent these losses because there is no way to remove a block once it has been added to the chain [56].

Blockchain to stop unauthorized access: There is a frequent connection between different nodes in many IoT applications. Only the party or node that is intended to receive this information can be accessed because of Blockchain's usage of publicly and privately issued keys for communication. The encryption of data is done with keys, meaning that the content will not be comprehensible to someone who cannot see it. The purpose of Blockchain data format is therefore to address the various security challenges encountered by apps that deal with IoT.

Blockchain architecture based on a proxy for resource constraint devices: Resource constraints pose a special challenge for the Internet of Things, despite the variety of security features that Blockchain offers in an interoperable environment. IoT devices are unable to store huge ledgers due to their severe resource limitations. Blockchain usage in IoT made easier by numerous efforts. One of the possible approaches for enabling IoT devices to use Blockchain is proxy-based architecture. To save the resources in an encrypted format, proxy servers can be installed on the network. With the help of the proxy servers, the client may download the encrypted data [57].

TABLE II. Blockchain solutions for IoT issues.

IoT Challenges	Description	Solutios through Blockchain
IoT Device Privacy	IoT devices have the potential to leak users' personal information.	To resolve this issue permissioned Blockchain can be used [44]–[46].
Data Usage	The data that is produced by the Internet of Things devices can be misused in an inappropriate manner, putting them at greater risk.	Blockchain helps to lock devices without authentication and if any modification is done then the system will reject it [47], [48].
Imperfect architecture	Many devices of IoT are vulnerable to a single failure point which affects the network and whole device both for retrieving the information or data.	Devices will be validated by Blockchain and data is varified cryptographically to make sure that originator has send the data to all nodes for availability when single point of failure is there [49].
Cost and Traffic	Handling the exponential growth in IoT devices.	Devices can directly connect and communicate with the peers through decentralization using Blockchain rather than centralization [50]–[52].
Heavy loaded cloud services and its inefficiency	Cloud services are not available due to power failure, various attack, bugs in software and other such problems.	Different nodes will update the records holding the same data due to which there is no single failure point as well as improved service efficiency [53], [54].

Removing centralized cloud servers: Because Blockchain ultimately gets rid of centralized cloud servers and converts them into a peer-to-peer network, it can improve IoT security. Data thieves focus primarily on centralized cloud servers. The encrypted data can be shared among each network node using.

IDoT (Identity of Things) and Governance : IoT (IAM) Identity and Access Management needs to handle a variety of complex difficulties in a quick, safe, and reliable way. The IoT device's identity and ownership is one of the main problems. Throughout its lifetime, a device's owner(s) can include the retailer, consumer, manufacturer, and supplier [58], [59]. The consumer's ownership of the device can be revoked or modified when an IoT device are compromised, sold again, or decommissioned. Another difficulty in managing IoT devices are their relationships and attribute management. Deployment GPS coordinates, Manufacturer, kind, make, serial number, location, etc. are some examples of a device's attributes. IoT devices have various connections like IoT devices to humans, IoT devices to ioT devices, and IoT devices to service interactions are examples of IoT relationships. An IoT device connection can include actions like deployment, use, shipping, sale, upgrade, repair, and sale.
This potential for swift, secure and effective solutions to these problems are offered by Blockchain technology. The use of Blockchain to provide authenticated registration of identity, track ownership and monitor asset is widespread. In order to allow for trust transactions and protect their integrity in a distributed environment methods such as TrustChain [60] are suggested. There's no exception with the IoT hardware. The Blockchain protocol can be used to authenticate and identify interconnected IoT devices using a set of characteristics and complex relationships that may be stored and retrieved in the Blockchain's distribution ledger.

Communicate Securely: Communication technologies for IoT applications like MQTT, HTTP, XMPP, or CoAP, also, protocols for routing like 6LoWPAN and RPL, are not by design security [61].To ensure secure communications, messages and applications should be embedded in other security protocols such as DTLS or TLS. Similar to how IPSec is frequently used to secure routing, 6LoWPAN and RPL protocols. IPSec, TLS, DTLS, and protocols of lightweight TinyTLS are labor-intensive and computationally complicated, memory needs, etc., which causes issues with centralized key management and distribution utilizing the PKI protocol. Key distribution and management are completely eliminated by Blockchain.A unique pair of GUID and asymmetric keys would be provided for each IoT device when it is installed and connected to the Blockchain network. This will also make it much easier to implement additional protocols for security, e.g. DTLS. Since DTLS, TLS, and IKE (or IPSec's IKE) does not require the handling and PKI certificates exchanged during the phase of a handshake, will be easier to invent lightweight security protocols that meet the needs of IoT devices' compute and memory

resources.

C. Challenges of Blockchain for IoT security issues.

This section discusses the Research gaps or challenges in deploying Blockchain for IoT security issues [62].

Scalability: It is crucial to examine current Blockchain technologies and schematize new ones for scalable IoT systems.

Lightweight architectures and schemes: For IoT systems, lightweight Blockchain-dependent architectures must be redesigned and improved to reduce the overhead of Blockchain. It is however necessary to certify that the security and privacy levels are as high as those of standard BC.

Processing Capability: Different IoT structures exist that have a wider potency range. In experimental frameworks, it might not be possible for all IoT nodes to conduct encryption. Alternative methods for the use of encryption with a group of IoT nodes or techniques that place minimal pressure on connected devices will therefore have to be available.

Storage: As there is no centralized controller in Blockchain, it's well suited for decentralized Internet of Things systems. However, it is still necessary to save the ledger which grows over time in every Internet of Things node. There may not be a great deal of data stored on the Internet of Things nodes.

Optimized design: A schematized IoT system must take BC-dependent privacy and security into account as an essential component. This may lead to an optimal systematization where computing, connectivity, privacy, coordination and security would be equally taken into account.

Lawsuit: Different countries and regions have different privacy and security laws. This feature is considered to be an important concern for the effective use of Blockchain technology in the Internet of Things systems. Before producers can provide privacy or security solutions, the typical case has to be used [63].

D. Related Work

Table III shows a summary of existing work regarding the secure Blockchain - IoT integration by addressing as well as achieving the security challenges. Different use cases with various proposed mechanisms for the incorporation of Blockchain in IoT has been listed out by achieving a certain level of security or privacy. In most of the paper certain security attacks has been simulated to test their proposed work. Different characteristics as well as limitations have been compiled that can lead to a number of possibilities to work further for mitigating the numerous security issues in IoT systems by integrating with Blockchain.

To investigate security issues related to the operation of an energy trading system, Aitzhan et al. [64] introduced the token-based Blockchain mechanism called PriWatt in the smart grid. Network-related attacks have been discussed, but the proposed solution has a single failure point, is expensive, and does not take privacy into account. The Blockchain-based PKI used by Axon et al. [65] has been used to manage the keys for secure device communication. Man in the Middle has been taken into consideration. But there are delays and storage problems in the proposed work. A particular level of privacy is not also being met.

In Blockchain gateway, according to Cha et al. [66], deals with various IoT devices on behalf of the user for communication by accepting and maintaining privacy policies. This method has problems with storage and scalability and achieves a coarse-grained level of decentralization. Dorri et al. [67] come up with Blockchain based IoT architecture handling most of the privacy and security threats in resource constrained IoT devices with constant performance overhead. Here No Proof of Work (PoW) is present and Qualitative overhead analysis is measured as a number of network clusters instead of network nodes. Vulnerability to the 51% attack, denial of service attacks, and modification attacks is not reduced. For previous Lightweight framework needs to be introduced for better mechanisms.

A lightweight BC framework for smart homes has been demonstrated by simulation in Dorri et al. [68], with the necessary security and privacy goals. in this work defense against Denial of service and linking attacks is also provided. But the performance overhead is there along with no privacy preservation. ChainAnchor, a Blockchain based architecture created by Hardjono et al. [69], stores transactions with data on device commissioning while maintaining privacy. IoT devices used are not designed with complete anonymity. By using smart contracts and policies, Lombardi et al. [70] develop an automated Blockchan-based system that conducts grid auctions. By reducing transaction costs, the method raises the degree of dependability, security, and accessibility. Here The method is not implemented or tested. Also, the problems with fraud and privacy are not mentioned. Scalability, economic impact, and technical viability have not been tested. Neha¨ı et al. [71] utilize Blockchain in a smart grid for peer to peer exchange of electricity along with optimizing transport. Energy consumption and privacy issues are not focused.

The FairAccess framework was created by Ouaddah et al. [72] to manage access control using a token-based system in constrained IoT devices. The main issue here is that only token-based authentication is used and to generate a token when it expires, two blocks must be mined. Shafagh et al. [73] created a Blockchain-based storage system to house and protect IoT data under the control and ownership of the

end user. The use of centralized key management results in persistent performance overhead as well as atomicity and robustness problems. The Enigma framework, developed by Zyskind et al. [74], uses distributed hash tables (DTH) for data storage, but it has a single failure point. Tsai et al. [75] proposed framework for an update of firmware using MQTT protocol and smart contract. Denial of Service (DOS) Attack is addressed but it is not simulated. In Refai et al. [76] manufacturers can manage updates of firmware for IoT devices using a Blockchain based security update system. 51% attacks and Denial of Service(DOS) attacks are simulated but firmware confidentiality is not attained. Lee et al. [77] It has been demonstrated how to update embedded IoT devices' firmware securely using a Blockchain. Attacks involving physical access and firmware modification have been addressed. Only supports a particular class of IoT devices, and it cannot defend from Firmware modification attack and Impersonation attack. The firmware over the Blockchain (FOTB) framework was created by Yohan et al. [78] for IoT firmware updates using Blockchain, taking into account modified firmware attacks, imitation attacks, MITM attacks, and replay attacks. However, in this case, the gateway simply forwards the update without verifying it. He et al. [79] introduce an Over The Air (OTA) Blockchain-based firmware update that addresses MITM and Denial of service attacks, but a wide range of IoT devices must be taken into consideration for testing. To connect identities to public keys, Pinto et al. [80] introduced a Public Key Infrastructure based on Blockchain connected with Keybase platform. Here, experiments on actual devices are not carried out. According to Singla et al. [81] proposal, there are several ways to manage certificates using Blockchain technology, while a Denial of services attack has been demonstrated but needs to extend the access control policies for IoT devices. In order to address DoS attack, Huh et al. [82] proposed Ethereum Blockchain based approach to manage devices in IoT. Here time taken for the process is higher and more storage is required. To manage and monitor IoT devices, Kostal et al. [83] developed a private blockchain-based approach. This approach can replace traditional PKI and improve monitoring capabilities. Javaid et al. [84], has proposed a trust model that uses the Proof of Authority (PoA) algorithm to check and add the information data in the block after recording the transactions data made by IoT nodes into the Blockchain.

Abbassi et al. [85] identifies a new secure distributed IoT architecture built on Software Defined Network (SDN) that uses Blockchain to address both current and foreseeable problems and satisfy the latest service requirements. The Blockchain SDN-IoT model's main goal was to create and deploy defenses, such as those for threat prevention, data protection, and access control, as well as to diminish network assaults like ARP spoofing, DoS attacks, and discover security issues. Tsengi et al. [86] provide a method that allocates a time restriction for each data processing and acquisition step; in this case, the evaluation of time is used to determine how to derive the Blockchain's data. Blockchain mostly improves scalability, reliability, and privacy in IoT addressing. The role and significance of Blockchain enabled technology in the IIOT environment has been highlighted by Yu et al. [87], the traceability, recoverability, and impact of IIoT-enabled industrial transactions on manufacturing for smart factories. A lightweight model of multi chaincode based on Blockchain technology is proposed to address issues related to Central supervisory authority governance that results in lack of privacy and insufficient scale, and single failure point Abdi et al. [88]. By including self executable smart contracts, this paradigm does away with Trusting Third Parties (TTP). The authors discussed how the suggested approach offers availability, integrity, and secrecy through a security study. An approach for decentralization and authentication of IoT device gateway has been proposed by Sarac et al. [89] where a basic interface is provided using Blockchain. IP mapping of network nodes is also provided and home server nodes collect all the data and do the monitoring of the devices with help of encrypted data securely forwarded by home routers.

A system of cross domain access controls providing safety and reliability is presented in the work of Rizzardi et al. [90]. The distributed access control shall be achieved using Blockchain and Networked Smart object middleware for managing the IoT data.NOS uses Message Queuing Telemetry Transport(MQTT) protocol for exchanging the information in IoT system. Zero knowledge proof approach along with the smart contract is proposed by Feng et al. [91] to share the data between data owners, cloud servers and cloud service providers. The proxy re-encryption method is used as a secure data sharing model to authorize all entities. To remotely monitor and warn farmers in real time, a Smart agriculture prototype is designed using cloud computing and Blockchain technology.

Chaganti et al. [92] addressed application using Ethereum Blockchain is built to store harmful data to stop attacks in the future. For evaluation of the assets and their provenance in IoT ecosystem, Vekantraman et al. [93] come up with secure ID management system based on Blockchain to handle the privacy and security issues in the IoT. For large enterprises, it is possible to further investigate the proposed prototype about extendability and adaptability as a huge amount of data has to be managed and monitored by storing it in the Blockchain. Another smart and distributed identity management system was proposed by Yin et al. [94] named SmartDID where the issues like deficiency of systematic proof system, resource limitation, security & privacy in IoT system are addressed. The authors have given the following thought: In order to hide data relating to privacy, a pair of credentials is created using cryptographic credentials and plain text. Furthermore, in order to ensure cryptographically secured credentials, the zero knowledge system is applied as a verification mechanism and commitment schemes are used for encryption. There's the possibility of Sybil attacks, and these methods won't be able to hide a link between attributes. There is, however, a Sybil threat and these meth-

TABLE III. Related Work

Papers	Security Challenges Addressed	Characteristics	Attacks Addressed	Limitations
Aitzhan et al. [64]	Confidentiality, Nonrepudiation, Authentication / ID Management	In decentralized Smart Grids, the trading security issues will be addressed through a system of Token BC built on PriWatt.	Network Related attacks	• Single failure point. • High cost and privacy breach [95]. • Simulation of some known network related attacks has been done out of identified attacks.
Axon et al. [65]	Confidentiality, Nonrepudiation, Authentication / ID Management	Blockchain based PKI is used to store and manage keys for secure communication bet devices.	Man in the middle attack	• Latency and storage issues [96]. • Lacks in certain level of privacy [97].
Cha et al. [66]	Confidentiality, Authentication / ID Management	BC gateway deals with different IoT devices on behalf of user for communication by accepting and preserving privacy policies.	—	• Scalability and storage issue. • Through this method, a lesser degree of decentralisation is attained than through the previous one.
Dorri et al. [67]	Confidentiality, Integrity, availability, Authorization, User Control	Blockchain based IoT architecture handling most of privacy and security threats in resource constrained IoT device with constant performance overhead.	(DOS) Attack, modification attack, dropping attack mining attack	• No PoW is present and Qualitative overhead analysis is measured in terms of number network clusters instead of network nodes. • Vulnerable to DOS attacks. • The 51 attack and Modification attacks is not reduced. • Lightweight framework needs to introduce.
Dorri et al. [68]	Confidentiality, Integrity, availability, Authorization, User Control	Lightweight BC framework for smart home has been demonstrated by simulation with necessary security and privacy goals.	Denial of Service (DOS) attack, linking attack	• Performance Overhead is there. • Privacy is not preserved.
Hardjono et al. [69]	Confidentiality, Authentication / ID Management	In a privacy preserving manner, the ChainAnchor architecture stores transactions in connection with commissioning the device.	—	• In many use cases of the Internet of Things where identification is required, the participating devices are completely anonymous and unable to be used [98].
Lombardi et al. [70]	Confidentiality, Integrity, availability	Automated Blockchain based system that make use of rules, auctions, and smart contracts in a grid. The system lowers transaction costs while enhancing security, availability, and dependability.	—-	• No realization or testing is done. • Privacy issues and fraudulent activity is not addressed. • No assessments were ever made of scalability, technical feasibility and economic impact depending on actual data. [99].
Nehaï et al. [71]	Confidentiality, Non-repudiation	Connect Blockchain and SmartGrid. The authors used Blockchain to help electricity trading while also enhancing its delivery.	—	• Energy consumptions needs to be considered. • Privacy issues is not addressed.

TABLE III. Related Work

Papers	Security Challenges Addressed	Characteristics	Attacks Addressed	Limitations
Ouaddah et al. [72]	Confidentiality, Integrity, Authentication / ID Management, Access control	FairAccess framework that is developed to manage token-based access control on constrained IoT devices.	—	• Token generation every time token expires.For new token 2 blocks is to be mined. • Only token-based authentication. • There is no recommendation for how to enable the use of relationships when providing access [100].
Shafagh et al. [73]	Confidentiality, Integrity, Authentication / ID Management	Blockchain based storage solution with safe end-user ownership of data and to guarantee control over their data for IoT data storage.	Sybil attack	• The performance overhead storage persists. • Relying on centralized key management or storage systems due to which it suffers from comparable issues with respect to atomicity and robustness against malicious service providers [96].
Wilkinson et al. Storj [101]	Confidentiality, Integrity, availability	Users can rent out their computer's unused hard drive space using the StorJ peer-to-peer protocol, which offers secure, private, and encrypted cloud storage.	Spartacus attack, or identity hijacking, Sybil attack, eclipse attack, hostage byte attack, Cheating Owner, Faithless Farmer, Defeated Audit attacks	• Problem of bloating remains [102].
Zyskind et al. Enigma [74]	Confidentiality, Integrity, availability, Authentication / ID Management	Enigma framework to develop data storage system using Distributed Hash Table (DHT) data structure.	—	• Single point of failure [103].
Vucinc et al. [104]	Confidentiality, Authentication / ID Management	OSCAR is an IoT end-to-end security architecture.	Replay attack, Denial of Service (DOS) attack	• Security aspects has not been considered.
Mettler [105]	Confidentiality, Integrity, availability, Authentication / ID Management, Non-Repudiation	Review of the effect of Blockchain technology on the Public Health Administration, Pharmaceutical Industry, User Based Medical research, and Drug Fraud.	—	• No practical implementation is there only different use cases has been discussed.
Tsai et al. [75]	Confidentiality, Integrity	Framework for managing updates of firmware using smart contracts and the MQTT protocol	Denial of Service (DOS) attack	• Attack is not simulated.
Refai et al. [76]	Integrity, availability	Firmware management for IoT devices using a Blockchain based security update mechanism for manufacturers.	DOS attack, 51 attack	• Confidentiality of firmware is not protected.
Lee et al. [77]	Confidentiality, Integrity, Availability	Firmware updates for embedded devices in an IoT are done using Blockchain.	Physical access attack, firmware modification attack	• Support a specific IoT devices. • Cannot protect from Firmware modification attack and Impersonation attack. • Security is not verified formally.
Pillai et al. [106]	Confidentiality, Integrity, Availability	PUSH based method and Hash Chain is used for firmware update in IoT devices.	Denial of Service (DOS) attack	• Experiments on real device need to be conducted.

TABLE III. Related Work

Papers	Security Challenges Addressed	Characteristics	Attacks Addressed	Limitations
Boudguiga et al. [107]	Confidentiality, Integrity, Availability	MultiChain used for firmware update in IoT devices.	DOS attack	• Verification of update not available.
Yohan et al. [78]	Integrity, Availability	FOTB framework is design for firmware update in IoT devices.	Impersonation attack, Firmware modification attack, replay attack and MITM attack	• The gateway forwards updates to IoT devices without verification.
He et al. [79]	Integrity, Authentication	OTA Blockchain based firmware update using hyper ledger fabric.	MITM attack, DOS Attack	• Needs incorporate diverse variety of IoT devices.
Pinto et al. [80]	Confidentiality, Authentication / ID Management	Identity and public key associations are made using a Blockchain based PKI connected to the Keybase platform.	—	• Experiments on real device need to be conducted.
Pavithran et al. [108]	Authentication / ID Management	Framework for managing IoT device public keys using Blockchain.	MITM attack, Phishing attack	• Confidentiality of data is not considered.
Singla et al. [81]	Integrity, Authentication / ID Management	For certificate administration, a Blockchain based Ethereum remote node, Emercoin and sync light node technique is utilized.	Denial of Service (DOS) Attack	• Needs to extend access control policies for IoT devices.
Gong et al. [109]	Confidentiality, Authentication, Integrity, Availability	Blockchain based device management for IoT network in smart city.	Denial of Service (DOS) Attack, malicious node injection, firmware forgery, Vendor Impersonation	• Need to extend reliable services as well as to carry out experimentation.
Huh et al. [82]	Confidentiality, Authentication	Ethereum Blockchain is used to manage IoT devices.	Denial of Service (DOS) Attack	• Time taken is more and needs to be improved. • Storage issues is there.
Kostal et al. [83]	Confidentiality, Authentication, Integrity	Managing and monitoring of IoT devices is being done by private Blokchain.	—	• Blockchain PKI can b integrated in place of traditional PKI. • Improvement in monitoring capabilities.
Javaid et al. [84]	Confidentiality, Authentication, Integrity	A Blockchain based model of trust that stores the data transactions made by IoT nodes on a decentralized ledger is proposed for the Internet of Things.	Sink Hole	• Does not support the auditing mechanism.
Abbassi et al. [85]	Confidentiality, Authentication, Integrity	Authentication, integrity, confidentiality, and the Blockchain The primary purpose of the SDN-IoT model was to develop and install defences, including those for threat prevention, data protection and access control.	Denial of Service (DoS) attacks, cache poisoning / ARP spoofing	• Security attacks are not demonstrated.

TABLE III. Related Work

Papers	Security Challenges Addressed	Characteristics	Attacks Addressed	Limitations
Tsengi et al. [86]	Confidentiality, Authentication, Integrity	Proposes the use of the Bitcoin Backbone Protocol (BBP) to act as a database for IOT	—	• No implemenetation on real time IoT applications.
Yu et al. [87]	Confidentiality, Authentication, access control	A scheme of increased security access in IIoT, which allow authentication and traceability has been suggested as part of smart factories.	collusion attack	• performance overhead is not mentioned. • Storage issue can occur in further run.
Abdi et al. [88]	Confidentiality, Availability, Integrity, Access Control	A auto enforcement policy system with on chain policy management is developed to eliminate the need of Trusted Third Party(TTP) by multiple chaincode based access control.	Denial of service and Distributed denial of service attack	• Network congestion and Latency are not managed properly.
Sarac et al. [89]	Confidentiality, Availability, Access Control	Basic interface for the security gateway architecture using Blockchain to provide authentication and decentralization offering IoT infrastructure with versatility and anonymity.	Man in the Middle attack	• Approach is of no use if database get corrupted. • Performance decreases because of increase in the number of IoT device.
Rizzardi et al. [90]	Confidentiality, Availability, Integrity, Access Control	Distributed and cross domain access control is achieved with combined help of Networked Smart object middleware and Blockchain.	Denial of service and Majority 51% Attack	• Testing with different types of Blockchain is not done to analyze performance.
Feng et al. [91]	Confidentiality, Availability, Integrity	A privacy protection approach depended on zero knowledge proof and smart contract is introduced for effective data usage.	Indistinguishability-chosen plaintext attack	• Implementation and evaluation of proposed work is not done. • Proposed work is depended on Trusted Third Party.
Chaganti et al. [92]	Confidentiality, Integrity, Access control	A smart farm security framework is proposed using Blockchain to prevent the future attacks by storing the malicious information.	Physical security attack, Data manipulation attack and Denial of service attack	• Implementation IoT gateway is missing.
Venkatraman et al. [93]	Confidentiality, Integrity, Availability	Prototype of ID management system based on Blockchain is introduced to address privacy and security in IoT.	–	• Large scale operation cannot be handled.
Yin et al. [94]	Confidentiality, Integrity, Availability, Access Control	SmartDID, a distributed Identity management system based on Blockchain's smart contract is proposed to address resource limitation and lack of proper proofing system in IoT.	Sybil Attack	• Proposed system leads to communication overhead leading to increasing latency and limited reliability.

ods are incapable of hiding attribute linkage. Therefore, a decentralized system in which several pseudonyms are used In order to tackle these issues, userIDs and one separate masterID are created and provided. Here Practical Byzantine Fault Tolerance (PBFT) consensus creates the communication overhead resulting in increase in latency and obstructing network transmission.

4. Discussion

For the sake of clarity for readers, it is necessary to provide you with a comprehensive understanding of the difficulties associated with integrating Blockchain and the Internet of Things, this paper surveyed the pertinent literature which is shown in Table III, security analysis for IoT systems has been done on various addressed security challenges such as Confidentiality, Authentication, Integrity, Availability, Identification Management, and Non Repudiation.

To resolve security issues in IoT different approaches are being proposed using the Blockchain but they are having some limitations such as single point of failure, communication as well as connection overhead, storage and performance overhead, latency issues, privacy preservation, storage issues and energy consumption. In place of Trusted Third Party or Interplanetary file systems for key management, Blockchain can be used as a core the component to store and manage keys of IoT devices with help of smart contract which can resolve a single point of failure. Also Strong authentication mechanism can be introduced using the Blockchain to prevent the IoT devices from being compromised as well as to stop malicious activities for better and more secure communication. Lightweight protocols and cryptographic techniques can be used in Blockchain to reduce the overhead and increase the performance in IoT systems.

An analysis of linked literature revealed that Depending on the desired results, use cases and technical challenges, there could be a number of different forms and methods for integrating Blockchain in the Internet of Things.Also, a variety of strategies that are highlighted in Table III to alleviate some of these problems were suggested by the research that was reviewed. In contrast to some who focused on a comprehensive architecture perspective that is needed for integration, others sought to minimize the challenges associated with them. As a result, an effective design that takes into account integration process challenges including IoT device constraints, privacy and security is becoming increasingly necessary. Blockchain is in an evolving stage which has its challenges. Therefore, while adapting the Blockchain for IoT these things should be taken into account.

5. Future Research Directions

Some points needs to be considered especially for the Blockchain whenever implementing it for IoT security which are mentioned in section 3. Some future research directions [110] have been listed in this field.

- How to use Blockchain to effectively identify various potential IoT threat vectors and to help take automated action plans against IoT threat vectors, while minimizing human interference?
- How can Blockchain be used to share and distribute publicly available IoT data sets that are important to IoT security research?
- How can Blockchain be used for detection and self-healing methods of corrupted firmware in the IoT environment?
- Design optimized platforms based on Blockchain and Blockchain to reduce energy consumption and provide more powerful and efficient services.
- How to use Blockchain and anti-forensic technology to prevent attackers from misusing the security functions of IoT devices to evade forensic investigations?
- How does the Blockchain guarantee the privacy and security of data generated and stored on publicly accessible IoT devices, especially when the IoT devices are controlled by adversaries?
- How can the Blockchain help to reduce the possibility that hardware and software for Internet of Things devices could be broken or corrupted if it is physically available?
- How to implement the most cost-effective and energy-efficient Blockchain based security solution in a strictly resource-constrained environment?

6. Conclusion

IoT gadgets of today lack security and defense mechanisms. This is mostly because of the limited resources in IoT, the inadequacy of developed standards, and the lack of secure developing and deploying hardware and software. Efforts to establish a coherent global strategy for the protection of layers of information technology are also impeded by the heterogeneous nature and diversity of Internet of Things resources. This paper examines and evaluates different aspects of security for sensors, networks, support or application layers as part of the Internet of Things. We have also covered numerous Blockchain potentials that can address and/or reduce various security concerns or dangers present in the IoT system. Additionally, the paper identifies and defines Open issues and research gaps that needs to be directed by the research fraternity to come up with reliable, efficient and scalable security solutions for IoT. Researchers can alleviate use of Blockchain in IoT security by making the automatic preventive and defending steps to identify or existing potential threats in IoT. Blockchain can also be used for detecting corrupted firmware and automatic self-healing of firmware in IoT systems by considering reduction in energy consumption with more efficient services. The energy efficient and cost effective security solutions based on Blockchain for IoT can be introduced by keeping the publically available IoT device's data safe and secure. This are the areas where the focus has to be done with more accurate and appropriate solutions can be obtained using Blockchain.

References

[1] W. H. Hassan *et al.*, "Current research on internet of things (iot) security: A survey," *Computer networks*, vol. 148, pp. 283–294, 2019.

[2] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[3] (2018) Flashpoint. mirai botnet linked to dyn dns ddos attacks. [Online]. Available: https://www.flashpointintel.com/blog/cybercrime/mirai-botnet-linked-dyn-dns-ddos-attacks/

[4] G. Yang, M. Jiang, W. Ouyang, G. Ji, H. Xie, A. M. Rahmani, P. Liljeberg, and H. Tenhunen, "Iot-based remote pain monitoring system: From device to cloud platform," *IEEE journal of biomedical and health informatics*, vol. 22, no. 6, pp. 1711–1719, 2017.

[5] J. Misra. (2017) Iot system — sensors and actuators. [Online]. Available: https://bridgera.com/IoT-system-sensors-actuators/

[6] (2017) Smart home blog. how to make your smoke detector smarter. [Online]. Available: https://www.smarthomeblog.net/smartsmoke-detector/

[7] (2019) Tictec bell. sensor d'ultrasons. [Online]. Available: https://sites.google.com/site/tictecbell/Arduino/ultrasons

[8] S. Kumar, S. Sahoo, A. Mahapatra, A. K. Swain, and K. K. Mahapatra, "Security enhancements to system on chip devices for iot perception layer," in *2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*. IEEE, 2017, pp. 151–156.

[9] C.-H. Liao, H.-H. Shuai, and L.-C. Wang, "Eavesdropping prevention for heterogeneous internet of things systems," in *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2018, pp. 1–2.

[10] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, 2005, pp. 46–57.

[11] G. Noubir and G. Lin, "Low-power dos attacks in data wireless lans and countermeasures," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 7, no. 3, pp. 29–30, 2003.

[12] S. H. Chae, W. Choi, J. H. Lee, and T. Q. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1617–1628, 2014.

[13] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 29–40, 2013.

[14] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of sybil attacks in wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 492–503, 2009.

[15] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," in *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*. IEEE, 2007, pp. 193–202.

[16] APWG. (2017) Phishing activity trends report. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2017.pdf

[17] C. Li and C. Chen, "A multi-stage control method application in the fight against phishing attacks," in *26th Computer. Security. Acaddemics. Communication*, 2011, p. 145.

[18] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[19] K. Weekly and K. Pister, "Evaluating sinkhole defense techniques in rpl networks," in *2012 20th IEEE International Conference on Network Protocols (ICNP)*. IEEE, 2012, pp. 1–6.

[20] F. Ahmed and Y.-B. Ko, "Mitigation of black hole attacks in routing protocol for low power and lossy networks," *Security and Communication Networks*, vol. 9, no. 18, pp. 5143–5154, 2016.

[21] A. A. Pirzada and C. McDonald, "Circumventing sinkholes and wormholes in wireless sensor networks," in *IWWAN'05: Proceedings of International Workshop on Wireless Ad-hoc Networks*, vol. 71, 2005.

[22] W. Wang, J. Kong, B. Bhargava, and M. Gerla, "Visualisation of wormholes in underwater sensor networks: a distributed approach," *International Journal of Security and Networks*, vol. 3, no. 1, pp. 10–23, 2008.

[23] M. Wazid, A. K. Das, S. Kumari, and M. K. Khan, "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 17, pp. 4596–4614, 2016.

[24] H. Kim, "Protection against packet fragmentation attacks at 6lowpan adaptation layer," in *2008 International Conference on Convergence and Hybrid Information Technology*. IEEE, 2008, pp. 796–801.

[25] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, "6lowpan fragmentation attacks and mitigation mechanisms," in *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, 2013, pp. 55–66.

[26] R. Riaz, K.-H. Kim, and H. F. Ahmed, "Security analysis survey and framework design for ip connected lowpans," in *2009 International Symposium on Autonomous Decentralized Systems*. IEEE, 2009, pp. 1–6.

[27] A. Dvir, L. Buttyan *et al.*, "Vera-version number and rank authentication in rpl," in *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*. IEEE, 2011, pp. 709–714.

[28] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, 2014.

[29] G. Wang, M. Mohanlal, C. Wilson, X. Wang, M. Metzger, H. Zheng, and B. Y. Zhao, "Social turing tests: Crowdsourcing sybil detection," *arXiv preprint arXiv:1205.3856*, 2012.

[30] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "A survey of middleware for internet of things," in *Recent trends in wireless and mobile networks*. Springer, 2011, pp. 288–296.

[31] Q. Zhang and X. Wang, "Sql injections through back-end of rfid system," in *2009 International Symposium on Computer Network and Multimedia Technology*. IEEE, 2009, pp. 1–4.

[32] R. Dorai and V. Kannan, "Sql injection-database attack revolution and prevention," *J. Int'l Com. L. & Tech.*, vol. 6, p. 224, 2011.

[33] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: a survey," *IEEE Internet of things journal*, vol. 3, no. 1, pp. 70–95, 2015.

[34] Acunetix. (2017) Insecure deserialization. [Online]. Available: https://www.acunetix.com/blog/articles/owasp-top-10-2017

[35] J. Kumar, B. Rajendran, B. Bindhumadhava, and N. S. C. Babu, "Xml wrapping attack mitigation using positional token," in *2017 International Conference on Public Key Infrastructure and its Applications (PKIA)*. IEEE, 2017, pp. 36–42.

[36] WS-Attacks. (2015) Attack subtypes. [Online]. Available: https://www.ws-attacks.org/XML_Signature_Wrapping

[37] S. N. Swamy, D. Jadhav, and N. Kulkarni, "Security threats in the application layer in iot applications," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, 2017, pp. 477–480.

[38] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive iot attacks survey based on a building-blocked reference model," *IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, pp. 355–373, 2018.

[39] OWASP. (2016) Top iot vulnerabilities. [Online]. Available: https://www.owasp.org/index.php/TopIoTVulnerabilities

[40] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, and M. A.

Spirito, "The virtus middleware: An xmpp based architecture for secure iot communications," in *2012 21st International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2012, pp. 1–6.

[41] C. H. Liu, B. Yang, and T. Liu, "Efficient naming, addressing and profile services in internet-of-things sensory environments," *Ad Hoc Networks*, vol. 18, pp. 85–101, 2014.

[42] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*. IEEE, 2015, pp. 180–184.

[43] S. Sayadi, S. B. Rejeb, and Z. Choukair, "Blockchain challenges and security schemes: A survey," in *2018 Seventh International Conference on Communications and Networking (ComNet)*. IEEE, 2018, pp. 1–7.

[44] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.

[45] P. Lv, L. Wang, H. Zhu, W. Deng, and L. Gu, "An iot-oriented privacy-preserving publish/subscribe model over blockchains," *IEEE Access*, vol. 7, pp. 41 309–41 314, 2019.

[46] U. Javaid, M. N. Aman, and B. Sikdar, "Blockpro: Blockchain based data provenance and integrity for secure iot environments," in *Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems*, 2018, pp. 13–18.

[47] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 12–18, 2018.

[48] U. Javaid, M. N. Aman, and B. Sikdar, "Drivman: Driving trust management and data sharing in vanets with blockchain and smart contracts," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*. IEEE, 2019, pp. 1–5.

[49] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for iot," *Ieee Access*, vol. 6, pp. 115–124, 2017.

[50] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *Ieee Access*, vol. 6, pp. 32 979–33 001, 2018.

[51] K. Valtanen, J. Backman, and S. Yrjölä, "Blockchain-powered value creation in the 5g and smart grid use cases," *IEEE Access*, vol. 7, pp. 25 690–25 707, 2019.

[52] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar, "Mitigating Iot device based ddos attacks using blockchain," in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 2018, pp. 71–76.

[53] K. R. Ozyilmaz and A. Yurdakul, "Designing a blockchain-based iot with ethereum, swarm, and lora: the software solution to create high availability with minimal security risks," *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 28–34, 2019.

[54] V. Sharma, "An energy-efficient transaction model for the blockchain-enabled internet of vehicles (iov)," *IEEE Communications Letters*, vol. 23, no. 2, pp. 246–249, 2018.

[55] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[56] D. He, S. Chan, and M. Guizani, "Security in the internet of things supported by mobile edge computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 56–61, 2018.

[57] O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, and F. Zanichelli, "Iotchain: A blockchain security architecture for the internet of things," in *2018 IEEE wireless communications and networking conference (WCNC)*. IEEE, 2018, pp. 1–6.

[58] I. Friese, J. Heuer, and N. Kong, "Challenges from the identities of things: Introduction of the identities of things discussion group within kantara initiative," in *2014 IEEE World Forum on Internet of Things (WF-IoT)*. IEEE, 2014, pp. 1–4.

[59] P. Mahalle, B. Anggorojati, N. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," *Journal of Cyber Security and Mobility*, vol. 1, no. 4, pp. 309–348, Oct. 2012.

[60] P. Otte, M. de Vos, and J. Pouwelse, "Trustchain: A sybil-resistant scalable blockchain," *Future Generation Computer Systems*, vol. 107, pp. 770–780, 2020.

[61] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[62] C. Ye, W. Cao, and S. Chen, "Security challenges of blockchain in internet of things: Systematic literature review," *Transactions on Emerging Telecommunications Technologies*, p. e4177, 2020.

[63] W. Ejaz and A. Anpalagan, "Blockchain technology for security and privacy in internet of things," in *Internet of Things for Smart Cities*. Springer, 2019, pp. 47–55.

[64] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, Sep. 2018.

[65] L. Axon, "Privacy-awareness in blockchain-based pki," *Cdt technical paper series*, 2015.

[66] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for ble-based devices in the internet of things," *IEEE Access*, vol. 6, pp. 24 639–24 649, 2018.

[67] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and solutions," *arXiv preprint arXiv:1608.05187*, 2016.

[68] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. IEEE, 2017, pp. 618–623.

[69] T. Hardjono and N. Smith, "Cloud-based commissioning of constrained devices using permissioned blockchains," in *Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security*, 2016, pp. 29–36.

[70] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri, and V. Sassone, "A blockchain-based infrastructure for reliable and cost-effective iot-aided smart grids," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018, pp. 1–6.

[71] Z. Nehaï and G. Guerard, "Integration of the blockchain in a smart grid model," in *The 14th International Conference of Young Scientists on Energy Issues (CYSENI) 2017*, 2017, pp. 127–134.

[72] A. Ouaddah, A. Abou Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in iot," in *Europe and MENA cooperation advances in information and communication technologies*. Springer, 2017, pp. 523–533.

[73] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of iot data," in *Proceedings of the 2017 on Cloud Computing Security Workshop*, 2017, pp. 45–50.

[74] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized computation platform with guaranteed privacy," *arXiv preprint arXiv:1506.03471*, 2015.

[75] M.-H. Tsai, Y.-C. Hsu, and N.-W. Lo, "An efficient blockchain-based firmware update framework for iot environment," in *2020 15th Asia Joint Conference on Information Security (AsiaJCIS)*. IEEE, 2020, pp. 121–127.

[76] R. Ahmed and W. Eugene. (2018) Blockchain for secure iot firmware updates. [Online]. Available: https://yoojeenwoo.github.io/EE209AS/

[77] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an internet of things environment," *The Journal of Supercomputing*, vol. 73, no. 3, pp. 1152–1167, 2017.

[78] A. Yohan and N.-W. Lo, "Fotb: a secure blockchain-based firmware update framework for iot environment," *International Journal of Information Security*, pp. 1–22, 2019.

[79] X. He, S. Alqahtani, R. Gamble, and M. Papa, "Securing over-the-air iot firmware updates using blockchain," in *Proceedings of the International Conference on Omni-Layer Intelligent Systems*, 2019, pp. 164–171.

[80] G. V. Pinto, J. P. Dias, and H. S. Ferreira, "Blockchain-based pki for crowdsourced iot sensor information," in *International Conference on Soft Computing and Pattern Recognition*. Springer, 2018, pp. 248–257.

[81] A. Singla and E. Bertino, "Blockchain-based pki solutions for iot," in *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 2018, pp. 9–15.

[82] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in *2017 19th international conference on advanced communication technology (ICACT)*. IEEE, 2017, pp. 464–467.

[83] K. Košt'ál, P. Helebrandt, M. Belluš, M. Ries, and I. Kotuliak, "Management and monitoring of iot devices using blockchain," *Sensors*, vol. 19, no. 4, p. 856, 2019.

[84] N. Javaid, "A secure and efficient trust model for wireless sensor iots using blockchain," *IEEE Access*, vol. 10, pp. 4568–4579, 2022.

[85] Y. ABBASSI and H. Benlahmer, "Bcsdn-iot: Towards an iot security architecture based on sdn and blockchain," *International journal of electrical and computer engineering systems*, vol. 13, no. 2, pp. 155–163, 2022.

[86] L. Tseng, X. Yao, S. Otoum, M. Aloqaily, and Y. Jararweh, "Blockchain-based database in an iot environment: challenges, opportunities, and analysis," *Cluster Computing*, vol. 23, pp. 2151–2165, 2020.

[87] K. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, "Blockchain-enhanced data sharing with traceable and direct revocation in iiot," *IEEE transactions on industrial informatics*, vol. 17, no. 11, pp. 7669–7678, 2021.

[88] A. I. Abdi, F. E. Eassa, K. Jambi, K. Almarhabi, M. Khemakhem, A. Basuhail, and M. Yamin, "Hierarchical blockchain-based multi-chaincode access control for securing iot systems," *Electronics*, vol. 11, no. 5, 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/5/711

[89] M. Šarac, N. Pavlović, N. Bacanin, F. Al-Turjman, and S. Adamović, "Increasing privacy and security by integrating a blockchain secure interface into an iot device security gateway architecture," *Energy Reports*, vol. 7, pp. 8075–8082, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352484721005448

[90] A. Rizzardi, S. Sicari, D. Miorandi, and A. Coen-Porisini, "Securing the access control policies to the internet of things resources through permissioned blockchain," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 15, p. e6934, 2022.

[91] T. Feng, P. Yang, C. Liu, J. Fang, and R. Ma, "Blockchain data privacy protection and sharing scheme based on zero-knowledge proof," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–11, 2022.

[92] R. Chaganti, V. Varadarajan, V. S. Gorantla, T. R. Gadekallu, and V. Ravi, "Blockchain-based cloud-enabled security monitoring using internet of things in smart agriculture," *Future Internet*, vol. 14, no. 9, 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/9/250

[93] S. Venkatraman and S. Parvin, "Developing an iot identity management system using blockchain," *Systems*, vol. 10, no. 2, 2022. [Online]. Available: https://www.mdpi.com/2079-8954/10/2/39

[94] J. Yin, Y. Xiao, Q. Pei, Y. Ju, L. Liu, M. Xiao, and C. Wu, "Smartdid: A novel privacy-preserving identity based on blockchain for iot," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6718–6732, 2023.

[95] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE transactions on industrial informatics*, vol. 14, no. 8, pp. 3690–3700, 2017.

[96] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[97] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2018.

[98] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for iot," *Computers & Security*, vol. 78, pp. 126–142, 2018.

[99] K.-L. Brousmichc, A. Anoaica, O. Dib, T. Abdellatif, and G. Deleuze, "Blockchain energy market place evaluation: an agent-based approach," in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. IEEE, 2018, pp. 321–327.

[100] O. J. A. Pinno, A. R. A. Gregio, and L. C. De Bona, "Controlchain: Blockchain as a central enabler for access control authorizations in the iot," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–6.

[101] S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin. (2014) Storj a peer-to-peer cloud storage network. [Online]. Available: https://www.storj.io/storj2014.pdf

[102] M. Dai, S. Zhang, H. Wang, and S. Jin, "A low storage room requirement framework for distributed ledger in blockchain," *IEEE Access*, vol. 6, pp. 22 970–22 975, 2018.

[103] E. Kokoris-Kogias, E. C. Alp, S. D. Siby, N. Gailly, L. Gasser, P. Jovanovic, E. Syta, and B. Ford, "Calypso: Auditable sharing of private data over blockchains," *Cryptology ePrint Archive, 2018/209, Tech. Rep.*, 2018.

[104] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "Oscar: Object security architecture for the internet of things," *Ad Hoc Networks*, vol. 32, pp. 3–16, 2015.

[105] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom)*. IEEE, 2016, pp. 1–3.

[106] A. Pillai, M. Sindhu, and K. Lakshmy, "Securing firmware in internet of things using blockchain," in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*. IEEE, 2019, pp. 329–334.

[107] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey, "Towards better availability and accountability for iot updates by means of a blockchain," in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2017, pp. 50–58.

[108] D. Pavithran and K. Shaalan, "Towards creating public key authentication for iot blockchain," in *2019 Sixth HCT Information Technology Trends (ITT)*. IEEE, 2019, pp. 110–114.

[109] S. Gong, E. Tcydenova, J. Jo, Y. Lee, and J. H. Park, "Blockchain-based secure device management framework for an internet of things network in a smart city," *Sustainability*, vol. 11, no. 14, p. 3889, 2019.

[110] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, 2018.

Nishant S Sanghani is currently pursuing PhD from Gujarat Technological University, Chandkheda, Ahmedabad, India. He has obtained his master's degree from Vyavasay Vidhya Pratishthan Engineering College, Rajkot, India and bachelor's degree from Dharmsinh Desai University, Nadiad, India. He is currently serving as an Assistant Professor in Information Technology Department at Shantilal Shah Engineering College (SSEC), Bhavnagar, India. He has authored and co-authored several number of papers in reputed national and international journals as well as conferences. His research interest are in Cloud Computing, Internet of Things (IoT), Blockchain and Network Security.

Dr. Bhavesh Borisaniya is currently working as an Assistant Professor in Information Technology Department at Shantilal Shah Engineering College (SSEC), Bhavnagar, India. He has obtained his doctorate and master's degree in Computer Engineering from Sardar Vallabhbhai National Institute of Technology (SVNIT), Surat, India and bachelor's degree from Government Engineering College, Modasa, India. He has authored and co-authored several number of papers published in reputed international journals and international conferences. His research interests are in Cloud Computing & Virtualization, Network Security and Machine Learning.