IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 25 January 2024, accepted 23 February 2024, date of publication 18 March 2024, date of current version 23 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3378592

SURVEY

A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and Applications

NATHALIE TAN YHE HUAN[1,2], (Member, IEEE), AND ZURIATI AHMAD ZUKARNAIN[2], (Member, IEEE)

[1]Department of Computer Network, Faculty Science and Information Technology, University Putra Malaysia, Seri Kembangan, Selangor 43400, Malaysia
[2]Faculty of Computer Science and Information Technology, University Putra Malaysia, Seri Kembangan 43400, Malaysia

Corresponding authors: Nathalie Tan Yhe Huan (gs67340@student.upm.edu.my) and Zuriati Ahmad Zukarnain (zuriati@upm.edu.my)

ABSTRACT By 2025, the Internet of Things (IoT) infrastructure is projected to encompass over 75 billion devices, facilitated by the increasing proliferation of intelligent applications. The IoT ecosystem consists of sensors that function as data generators and applications that necessitate financial transactions to compensate the data producers. Security is a highly important concern. Typically, IoT gadgets are vulnerable to security breaches, and the advancement of industrial systems might introduce severe security weakness. The rapid evolution of IoT technologies and deployment scenarios makes the existing research challenging to keep pace with emerging threats and vulnerabilities. Employing blockchain technology makes it feasible to enhance security by maintaining payments in a ledger that is not just secure but also translucent, distributed, and immutable. This article provides an introductory overview of the IoT and subsequently delves into the many security threats and vulnerabilities arising within the IoT framework. This study provided an overview of the blockchain, focusing on its categorization and important properties. Moreover, this article examines the necessity of combining blockchain technology with the IoT, in addition to reviewing relevant literature and the studies conducted by other scholars. This article offers insight into the uses of blockchain on the Internet of Things (IoT).

INDEX TERMS Blockchain, integration with IoT, blockchain characteristics, IoT security issues.

I. INTRODUCTION

The term Internet of Things (IoT) refers to the physical network device integrated with sensors and software to communicate and share data with other inter-connected devices and systems. IoT applications have grown significantly in the last several years, and experts predict there will be 20 billion linked IoT devices by 2025 [1]. IoT devices may vary from smart home usage to advanced industrial standard instruments, including smart vehicles, smart buildings, health monitoring, production management, wearable technology, and smart grid [2]. It also refers to a real-time information-sharing system for items that use product electrical coding and radio-frequency identification (RFID) based on Internet technology [3]. Through the integration of information and communication technologies like sensors and cloud computing, IoT has progressively grown into an information industry chain. Currently, Industry 4.0, smart society, artificial intelligence (AI), and 6G represent some of the areas in which the Internet of Things has penetrated daily life. The Internet of Things (IoT) constitutes a network that interconnects a multitude of devices, including laser scanners, RFID readers, infrared sensors, and global positioning systems. To intelligently identify, find, track, monitor, and administer the complete network, the system links any device that may be used to the Internet for information exchange

The associate editor coordinating the review of this manuscript and approving it for publication was Tawfik Al-Hadhrami.

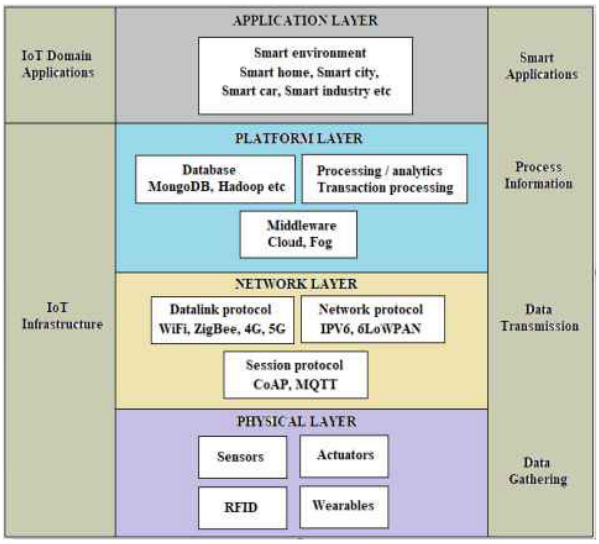

FIGURE 1. IoT architecture.

and communication [4]. Figure 1 shows that there are four levels comprising the framework of the Internet of Things: the physical layer, the network layer, the platform layer, and the application layer.

As mentioned earlier, IoT devices are widely used to manage and handle enormous amounts of sensitive and confidential data. As a result, these devices have been a target for hackers and cybercriminals. Hackers may make use of IoT devices to steal private data, including bank card information, location data, and financial accounts. However, there is a lack of recognition for these security demands. Moreover, it has been revealed that over 25% of botnet attacks came from IoT devices such as household appliances [5]. Additionally, many websites have been attacked by Distributed DDoS attacks, which also started from IoT devices, including Twitter, Netflix, and Spotify. Corporate investment in IoT-related information security is anticipated to rise from $83.5 billion to $119.9 billion by 2021. To raise the overall security level of IoT, it is essential to employ adequate technologies. As a result of the blockchain's rapid growth, its security features which include its decentralized and transparent system, consensus and privacy protocols, encrypted data and management, and smart contract agreements—have been brought to lightweight and become practical strategies for Internet of Things security.

Basically, Blockchain refers to a network of interconnected digital blocks that function as an open distributed ledger. Their distinctive characteristics encompass security and decentralization, which ensure a permanent record of sensor data in blockchain-based transactions to provide a verification trail of sensor observations. Data traceability and irreversible alteration are guaranteed by the time stamp mechanism of the certificate value and the safe transmission of the hash chain-based encryption technique [6]. Consistency strategies are utilized to guarantee the link between the node and the block data. The blockchain is a highly effective security solution, relying on consensus, communication technology, and encryption. Blockchain is revolutionizing the IoT network in several ways. IoT might comply with greater security requirements because of blockchain's unique characteristics, including its untampered data, open and transparent multiparty consensus, and peer-to-peer decentralized network [7].

Additionally, there are several kinds of Blockchain according to the usage, which are public, private, and consortium. Public blockchain enables open access and control to everyone in the network. In contrast, the private blockchain restricts access to only invited individuals. The consortium blockchain is between public and private [8].

Hence, we performed an extensive examination of the existing literature, encompassing 119 scholarly papers from 2016 to 2021, in order to present the most current and advanced research in this field. We have comprehensively analyzed the available literature by comparing, contrasting, and critically analyzing it. Through this process, we have identified the present issues and future research paths, specifically focusing on the aspect of lightweightness. Section I briefly introduced Internet of Things (IoT) with the IoT architecture. In Section II, a few security issues are raised in the IoT according to the IoT architecture layer. Next in Sections III, IV, and V are the discussions on blockchain overview, classification, and key characteristics, respectively. Furthermore, Section VI discussed the need to integrate blockchain into IoT fields, and then Section VII reviewed the blockchain-based IoT applications.

II. SECURITY ISSUES IN IoT ARCHITECTURE LAYER

The number of Internet of Things (IoT) devices is growing, and because these devices lack security, they have become a breeding ground for hostile activity [9]. In this particular review work, a commonly used four-layered design is taken into consideration [10]. As mentioned before, there are four levels that comprise the Internet of Things architecture environments (Figure 1). As different technologies are used at each of these levels, a range of problems, security risks, and dangers arise.

A. PHYSICAL LAYER

The physical layer handles sensors on data information collection from the environments [11], [12], [13]. To collect data from the environment, sensors can take various forms, including mechanical, electrical, electronic, chemical, or smoke detectors, as well as ultrasonic, temperature, and video sensors. Nodes, an alternative term for sensors, are susceptible to node-capturing attacks, in which a malicious node is substituted for the original node or the node is captured. The attacker can introduce malicious or fake code into the node through an over-the-air firmware or software upgrade, resulting in incidents of fake data injection incidents or fraudulent code injection [14]. There is no built-in security at all for these sensors and actuators.

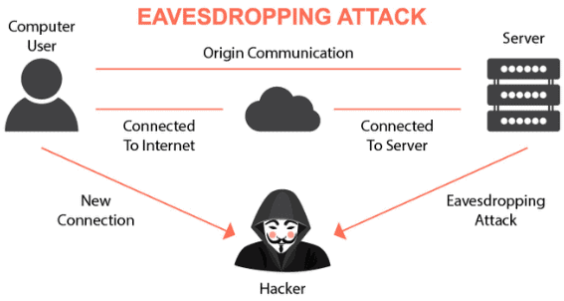

FIGURE 2. Eavesdropping attack.

This layer is vulnerable to side-channel attacks based on time, power consumption, and laser [15]. Nodes in an unsecured environment are vulnerable to eavesdropping attacks during data transfer or other related activities [16]. Because IoT devices have limited power, hackers take advantage of this by depleting the power supply and preventing sleep. IoT devices usually activate their security mechanisms after booting, which allows an attacker to initiate an attack at this period.

1) EAVESDROPPING ATTACK

Inadequate authentication and data transfer across several nodes might allow eavesdroppers to acquire confidential information [17]. Eavesdropping is defined as the practice of hackers listening in on private communications within a wireless network in order to obtain such information [18].

Various nodes placed in open spaces serve as the foundation for Internet of Things applications. They are therefore susceptible to eavesdroppers. At many stages, such as data transfer or authentication, hackers might listen in to steal information [19].

One way to minimize such attacks at the physical layer is to ensure that devices are authenticated. Consequently, for physical devices inside the Internet of Things networks to be considered properly recognized in the system, they must authenticate themselves before transmitting and receiving data. As a result, the network will be inaccessible to any hostile devices. Moreover, we can distinguish between two secure functions in an IPSec Security channel: encryption and authentication. By using encryption, this system can stop node tempering assaults and eavesdropping.

Consequently, the recipient can determine if the person sending the information over IP is authentic or fraudulent. Further, to ensure reliability, secrecy, and confidentiality in intelligent environments based on the Internet of Things (IoT), it is essential to include certain security measures such as cryptography, error detection, and risk evaluation to mitigate the danger of data breaches [20].

2) MALICIOUS CODE INJECTION ATTACK

Malicious code injection into the memory of a node is termed malicious code injection, also known as MCI or fake data injection attacks [14], [19]. These nodes may be used as a gateway for a variety of unauthorized activities, including providing false information and breaking into or taking over a whole Internet of Things network. The attacker inserts malicious code into the memory of the node in this attack. It could use malicious code to make nodes carry out unwanted tasks or even take over the entire IoT system [21]. Through this attack, the attacker can access the network, deplete its resources, and ultimately stop providing services. Potential attackers may attempt to gain control of a specific node inside the Internet of Things system, replacing it with another harmful counterpart or inserting an illegitimate among the nodes [22]. Upon acquiring control of the newly discovered node, which seems to be a constituent of the system, the assailant can infiltrate the network and govern the entirety of network data transmission. This has the potential to compromise the overall security of IoT applications [23].

3) SLEEP DEPRIVATION ATTACK

The term ''sleep deprivation attack'' (SDA) describes the process of low-powered nodes' batteries running low and their subsequent denial of service [19]. The goal can be accomplished by inserting malicious algorithms with endless iterations into the edge devices. This might drain the batteries and result in an attack that causes insufficient sleep.

The Internet of Things (IoT) uses a lot of gadgets that need to have their batteries changed often to maintain great performance and a longer lifespan. This may be used by adversaries to keep the sensor nodes awake or to run malicious code that causes the devices to perform indefinite loops, increasing the consumption of power [24].

The majority of IoT network nodes in distant locations are run by swappable batteries; to extend the life of the batteries, these nodes are designed to enter a sleep mode while not in use. By providing the node with incorrect input, the attacker in this attack keeps it awake and prevents it from entering sleep mode, which causes power consumption and node termination.

B. NETWORK LAYER

This layer relies on foundational networks, for example, wireless sensor networks, the internet, and communication networks. Its main job is to transfer the information gathered from the physical layer to the processing computing unit [25]. Information from the physical layer is sent to the computing unit via the network layer for additional processing. This layer is extremely prone to attacks using several Internet of Things devices [26]. A scam called phishing aims to take over several Internet of Things devices [27]. An assailant employing fraudulent requests endeavors to overwhelm the target in a DDoS attacks. During DDoS attacks, IoT devices are utilized as botnets to produce an overwhelming surge of requests, therefore obstructing the target's access to more resources [28]. Examples of routing attacks include wormhole and sinkhole attacks consisting of the attacker gaining access to nodes to reroute traffic onto an alternative path [29].

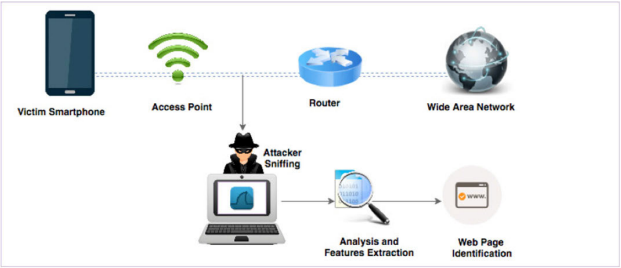

FIGURE 3. Traffic analysis attack.

1) TRAFFIC ANALYSIS ATTACK

During this assault, the assailants use packet sniffers or port scanning to gather network information and subsequently analyze user device network traffic to collect sensitive user data. This is a subtle attack that is challenging to identify [30]. In the collection of sensitive data, such as RFID, wireless communication systems are sniffed. In these situations, hackers use packet sniffers or port scanning software to initially gather network-related information before launching an assault on the targeted data. To stop unwanted access to data on sensor nodes, two network layer countermeasures are employed: authentication methods and encryption techniques.

In addition, the encryption of data sent to and from different IoT sensor nodes depends on using a range of secure routing algorithms to ensure routing security. For instance, employing several channels enables safe routing, corrects network issues, and boosts system efficiency. Wormhole attacks are one type of attack that the secure routing protocol Ad hoc (AOMDV) can handle.

2) SNIFFING ATTACK

Through the use of sniffing software, attackers can gather information about network traffic and occasionally divulge login credentials, leaving a system extremely exposed. In the absence of security measures, the attacker can obtain sensitive data [31]. Confidential data is compromised during a sniffing attack, which is carried out with the use of sniffing tools and network traffic data [32]. It's an attack whereby network packets are listened in on. This attack puts the secrecy of communications at risk and is widespread in both wired and wireless networks. An attacker can use a compromised device or directly capture packets from the shared media to carry out this attack. Sniffed packets may provide topological information, route information, and data content [33].

3) ROUTING ATTACK

Redirecting communication channels while data is being sent is referred to as a routing attack [19]. One of the most well-known types of routing assaults is the sinkhole attack, in which nodes are drawn in by artificial displacement pathways, creating a more practical communication channel [34]. The wormhole attack is a sort of routing attack that enables a rapid transmission channel between two

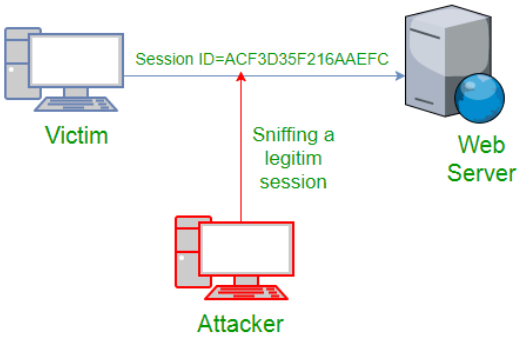

FIGURE 4. Sniffing attack.

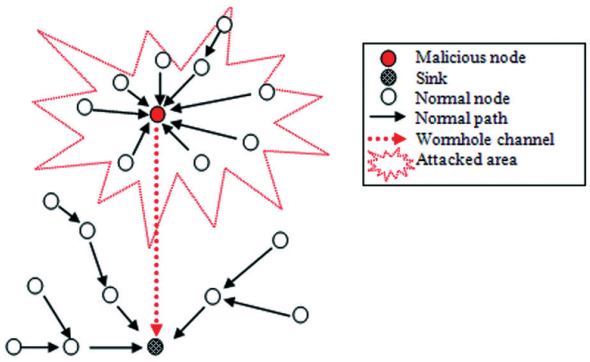

FIGURE 5. Sinkhole attack.

nodes [35]. An attacker can circumvent security measures by deliberately creating a tunnel of malware between a network node and another device. Examples of routing attacks include worm-hole and sinkhole attacks, in which the attacker attempts to redirect traffic to another path by obtaining access to nodes [29]. Wormholes can pose a serious danger to the Internet of Things system when used in conjunction with other techniques [19].

4) DDOS ATTACK

DoS attacks are consciously designed to interfere with, corrupt, or restrict access to network data for legitimate users, disrupting user services using excessive network traffic and malicious packets [36]. Between the years 2019 and 2021, distributed denial of service (DDoS) assaults gained a significant amount of momentum as a direct result of the broad deployment of COVID-19 [37]. Figure 3 demonstrates the scenarios of DDos attacks whereby the attackers transmit a large volume of data at an uncontrollable rate, thus breaking the system and sending maliciously structured packets that the recipient user side cannot manage. The goal of an attack using DDos is to infect devices, which are also referred to as zombies [38]. This attack exposes a system to security risks, posing serious network security difficulties. Due to its uncomplicated structure and user-friendly interface, DDoS assaults, whether from a single or numerous sources, may be easily carried out and inflict significant damage on a targeted system. These attacks do not require much expertise, talent, or resources. DoS attacks can seriously harm the system in

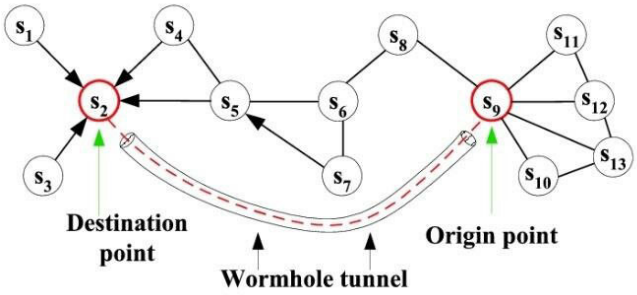

FIGURE 6. Wormhole attack.

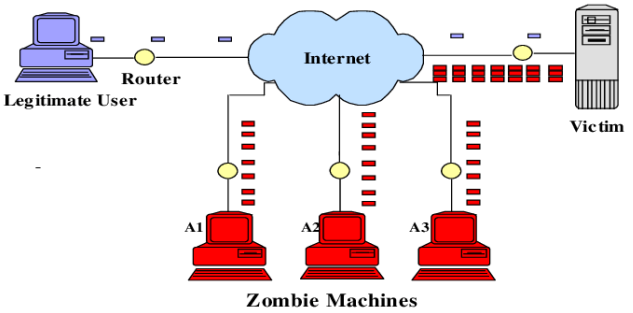

FIGURE 7. Scenarios of DDos attack.

terms of operating expenses even when they do not result in any loss of sensitive data.

The objective of this attack is to disrupt the availability of a server in an Internet of Things (IoT) network by overwhelming the communication channel with fraudulent requests originating from several IoT devices [28]. Their vulnerability stems from the complexity and heterogeneity of IoT networks at the network layer. Due to their occasionally inadequate security configurations, a significant number of IoT devices utilized in IoT applications are ideal targets for DDoS attacks on target servers.

DoS attacks use cryptanalysis to overwhelm target servers with an overabundance of unauthorized requests, rendering the server unable to reply [39]. Second, it causes a denial of service by interfering with the server's ability to interact with legitimate nodes. Distributed-DoS attacks are those that overload underlying servers with traffic from various sources. Despite the sufficient complexity and variety of IoT systems, DDoS attacks can still occur at the network layer. Because of the devices' and apps' poor settings, attackers can get gateways to execute DDoS assaults against the servers. A similar kind of assault occurred during the 2017 Mirai botnet attack [39].

C. PLATFORM LAYER

In between the network and application layers is the platform layer or support layer. This layer facilitates computation, data storage, and resource allocation. Numerous services have been generated by IoT devices when they connect and exchange data. The primary function of the platform layer is to provide robust computational and storage capabilities. Consequently, it has the capability to store data from the underlying layer in libraries and then retrieve, analyze, compute, and make determinations based on the results of the calculations [40]. At this layer, ensuring database security is of paramount importance due to its vulnerability to DDoS, Man-in-the-Middle, and SQL injection attacks. The MQTT protocol serves as a broker in the communication process between the service provider and the customer. An attacker that manages to take over the broker gains control over all communication in a man-in-the-middle attack [41]. This layer is exposed to numerous types of threats that could take over the entire Internet of Things application by infecting the middleware. Since access to data is typically the goal of an attack at the platform layer, database, and cloud security are essential in this layer.

1) SIDE CHANNEL ATTACK

The type of attack works by looking into the algorithmic implementation's accessible side features, such as power use, processing timing, related noises, etc. A lack of safe ways to handle and store IoT data, such as putting unencrypted data on IoT devices or the cloud, might lead to this kind of assault [42]. Attackers observe and examine the physical performance and information leakage of the nodes to crack the network encryption and secret key. A variety of factors, such as electromagnetic emission, execution time, and power consumption, are included in the physical performance. In some situations, sensitive information leaks are the attackers' goal, not the nodes themselves [19]. Advertisers target the intricate structures of processors, electromagnetic radiation, and resource use to obtain confidential data. Side Channel Attacks (SCA) may be classified as timing-based or laser-based, depending on the level of power used. The security against side-channel attacks (SCA) in modern electronics designs mostly relies on implementing cryptographic techniques on recently developed field-programmable gate array (FPGA) devices.

2) STORAGE ATTACK

Large volumes of data, including personal information, must be kept in the cloud or on storage devices in IoT-based smart environments. These locations are vulnerable to attacks that might corrupt or alter the data. Attack surfaces become more widespread as a result of data replication and accessibility to a wider range of users [43].

3) SQL INJECTION

Structured Query Language (SQL) injection is the process of introducing nefarious commands into software [44], [45], and [45] in order to obtain and modify user-sensitive data. SQL injection was identified as the leading online security issue by the Open Web Application Security Project (OWASP) in 2018. An SQL database processes the query that the attacker submits into an exposed field. There is an issue like this in many kinds of systems, including the Internet of Things. The primary problem with SQL injection is its

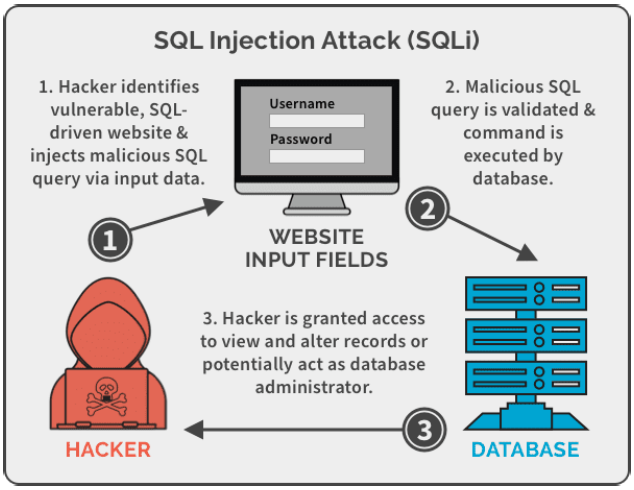

FIGURE 8. SQL injection attack.

potential to cause privilege escalation, which would give the attacker more access to the system [46].

D. APPLICATION LAYER

This is the top layer of the protected Internet of Things architecture, responsible for delivering consumers services and apps that are clever and smart in accordance with their requirements. Smart applications, such as those for smart homes, cities, and healthcare, are found on the application layer. Privacy and data theft are significant issues since this layer interacts directly with end users [47]. The malicious code injection attack also affects this layer, similar to its effects on other levels. Because it disrupts services, a service interruption attack is comparable to a DDoS attack. While certain individuals have the special ability to provide authorized users access during an attack, if this access is compromised, the entire system may be vulnerable to attack [48]. Confidential data is compromised during a sniffing attack, which is carried out using sniffing tools and network traffic data [32].

1) BOTNET ATTACK

A botnet attack is a type of cyberattack where the attacker searches a network for weak or poorly secured Internet of Things (IoT) devices. In this attack, attackers will be able to take control of internet-enabled devices, such as computers, tablets, etc., without the owner's authorization and perform malicious activity [49]; they mainly target insecure (IoT) devices and use malware to embed a bot software into them after analyzing the scanning data [50]. The installed bot application links the hacked systems with a peer network or central server. Through this connection, it sends commands to carry out various harmful tasks, such as transmitting spam [51]. The botnet attack poses a critical risk to the whole internet in addition to being a major hazard to unprotected Internet of Things devices. Since the start of the Mirai botnet attack in 2016, there has been a continued rise in IoT botnet attacks. Numerous variations and clones of the Mirai botnet have

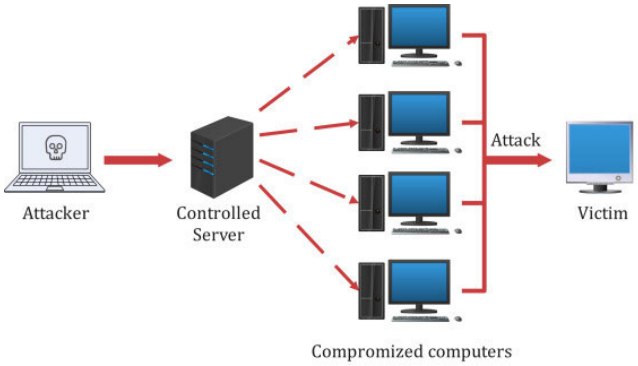

FIGURE 9. A schematic of botnet attack.

emerged since the source code was available [52]. Figure 1 shows the schematic of the botnet attack.

2) MAN-IN-THE-MIDDLE (MITM) ATTACK

The Man-in-the-Middle (MitM) attack is the most common attack in IoT, which involves intercepting node-to-node traffic to acquire sensitive data, including authentication credentials [53]. It interrupts communication by hiding the user's identity.

For instance, node A may attempt to communicate with consumer X while consumer X is engaged in correspondence with the MiTM attackers pretending to be end-user X. This poses substantial security vulnerabilities as there is a high likelihood that the attacker will acquire data breaches [54]. In this way, the attacker will be able to take over the communications and spread misleading data [55]. Using fake sensor data to damage physical assets and corporate activities is one example of MitM in the IoT space. A fake website was sent to 2.5 million users of the Equifax website, a well-known example of the MitM. Figure 2 illustrates the schematic of the MitM attack.

3) DDoS ATTACK

Distributed Denial-of-Service (DDoS) attacks pose a significant threat as they have the potential to render internet services inaccessible to authorized users. According to the latest information from Microsoft, there appears to be a threefold increase in DDoS attacks. The notable distributed DDoS attacks in 200 were the Amazon Web Services (AWS) attack, the attacks on GitHub DDoS attack, the Dyn DDoS attack that resulted in harm to internet services, and the Mafiaboy strikes [56]. To execute such attacks, hackers utilize several techniques, primarily relying on botnets, to overwhelm the servers of the targeted website or service with a substantial flood of data, overwhelming their ability to process legitimate requests. The frequency of distributed denial of service (DDoS) traffic has been a major hindrance during the past decade since it greatly impairs network communication efficiency. The current defense solutions mostly focus on mitigating the effects of DDoS attacks by targeting the service aspect, hence making these problems inherent to the system [57].

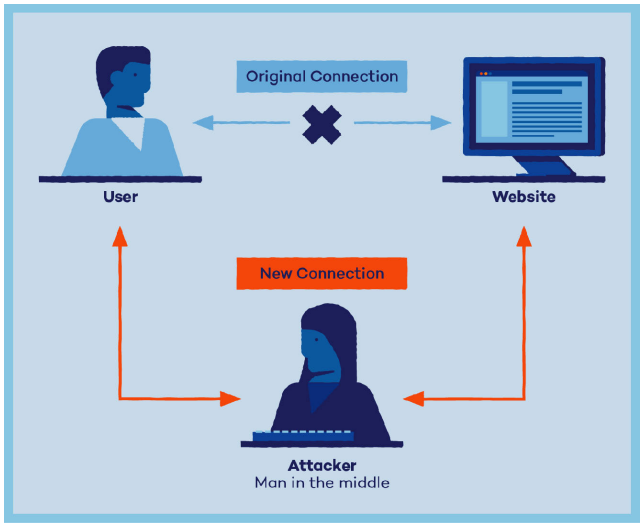

FIGURE 10. Man-in-the-Middle (MitM) attack.

Upon initiation of a DDoS attacks on an Internet of Things network, the system promptly begins assigning resources to manage the influx of requests. Even if a legitimate user were to submit more requests, they would be denied, impeding the IoT network's proper operation [58]. To tackle this problem effectively, it is important to implement sophisticated security measures that safeguard IoT networks. The main obstacles in adopting an attack detection technique are the limited power, computation, bandwidth, and capacity for storage resources at different levels of the Internet of Things (IoT) architecture [59].

III. RELATED WORKS

Yazdinejad et al. presented and created a safe intelligent fuzzy blockchain framework that makes use of fuzzy concepts to identify security risks in blockchain-enabled Internet of Things networks. They evaluated multiple models and contrasted the outcomes using the standard adaptive neuro-fuzzy inference system algorithm and fuzzy classifiers. Moreover, validation of transactions has used the fuzzy string-matching technique to extract fraud detection signals. Both throughput and latency are efficiently handled by the suggested architecture. Based on the degree of security danger, fuzzy control systems have proven useful in identifying threats in blockchain-enabled Internet of Things networks [60].

Yazdinejad et al. designed the Block Hunter framework, which uses Federated Learning (FL) techniques to search for abnormalities in blockchain-enabled IIoT smart factories. In order to cut down on resources and boost the throughput of blockchain-enabled IIoT network searching, the Block Hunter employed a cluster-based design. A range of machine learning (ML) techniques were used to assess the Block Hunter framework in order to find abnormalities. They also looked at how the Block Hunter performed in relation to the block size, block production interval, and various miners. Their findings show how well the model performs in automatically searching for abnormalities while protecting the

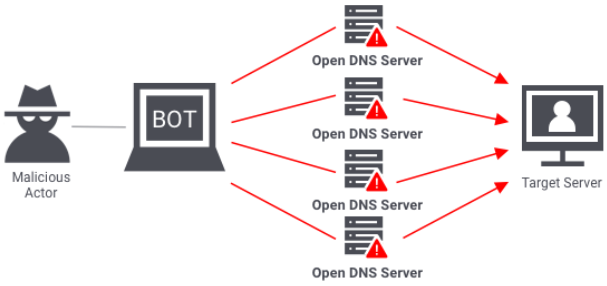

FIGURE 11. DDoS attack.

privacy of user data [61]. Other than that, Yazdiejad et al. also performed a study on another work which developed an advanced authenticating technique in 5G network to safeguard privacy and offer intelligent control across diverse cells with the use of SDN structure and blockchain technology. As the results showed, minimal latency was achieved for the 5G network by eliminating the recurrent manipulations among heterogeneous cells. Additionally, the enhanced Delegated Proof of Stake (DPOS) consensus algorithm linked to the Blockchain Center (BC) proved to be a better fit for scalability and improved energy usage with a lighter blockchain as opposed to using the Proof of Work (POW) [62].

O Mounnan et al. suggested a new architectural model that uses blockchain technology to allow access control in Internet of Things (IoT) using fog computing. The suggested method provides a new approach to a number of problems, including storing information, carrying out transactions and tasks to build trust in an open environment. They used smart contracts to spread the policy throughout the blockchain network, ensuring the execution of the identity and authentication processes. If the users align with the policy, access is authorized. As a result, the suggested approach offers security, privacy, and authentication at scale without the need for an intermediary third party [63].

Peyman et al. demonstrated a specified blockchain architecture within Internet of Things (IoT) systems and the proposal of a security protocol created explicitly to enhance privacy and facilitate anonymous audits, this has brought a spotlight on these difficulties. With a focused emphasis on overcoming the inherent security difficulties, they had offered useful insights into the design and operational dynamics of blockchain-based Internet of Things (IoT) systems. The suggested security protocol is an essential factor in strengthening these systems since it places a high priority on maintaining privacy-enhancing techniques and the integration of technology. Comparison was made had shown the approach towards stability and effectiveness, differentiating it from other approaches [64].

IV. BLOCKCHAIN OVERVIEW

Blockchain creates an unchangeable audit trail by storing the IoT sensor data such as payment history, personal information, and contracts as blockchain transactions [65]. It is generally made up of several time-stamped transactions managed

by sophisticated algorithms [66]. Blockchain technology was first presented to address the issues of cryptocurrency double spending [67]. Blockchain technology's security, auditability, and anonymity have prompted a lot of demand [68]. The transaction headers are disclosed to the public and are neither possessed nor mediated by any particular person or organization, even though the blocks are heavily encrypted and anonymous [69].

Blockchains consist of three main components: blocks, chains, and networks. It uses cryptographic techniques to store transactions in a series of blocks [70]. Every block in a blockchain, except for the initial block, uses the parent block's hash value as an inverted reference to point to the block that came just before it (parent block) [8]. There isn't a parent block for the genesis block, the first block in a blockchain. Figure 3 shows the blockchain block structure, which consists of the following information:

1. Blok header – contains block version, which indicates the validation rules to follow.
2. Previous block address – hash of parent block
3. Timestamp – record the current time (seconds)
4. Nonce – increased by each hash calculation, starting from 0.
5. Merkel root – hash value of the root of the Merkel tree

A blockchain expands as transactions are completed, and every node in the network verifies the newly created blocks.

It will then be added to the blockchain's end [71].

V. BLOCKCHAIN CLASSIFICATION

Blockchain technology is classified into three categories: public, private, and consortium blockchain.

A. PUBLIC BLOCKCHAIN

Everyone can take part in the public blockchain technology since it does not require authorization. Consequently, each participant possesses the capacity to execute transactions and participate in the consensus mechanism for block formation. Additionally, all participants in the blockchain have the ability to observe transactions, but their identities remain concealed. The public blockchain has a low throughput, indicating it can only execute a limited number of transactions per second. It is entirely decentralized, and every node has the ability to participate anonymously without the need for registration, authorization, or authentication [72]. Some of the technologies that are associated with cryptography are digital signatures, hashing [73], symmetric/asymmetric keys [74], and ECDSA [75]. These technologies are utilized to guarantee that transactions cannot be altered. These individuals are motivated by economic incentives such as transaction fees and prizes.

However, it can grow to accommodate a high number of nodes for processing transactions. In order to find solutions to this problem, such as sharding, off chains, and other approaches, a lot of research is being done [76] and [77]. There are various problems associated with public blockchain, including performance, privacy, and security. However, public blockchain is extremely decentralized. Two of the most well-known platforms for public blockchains are Bitcoin and Ethereum.

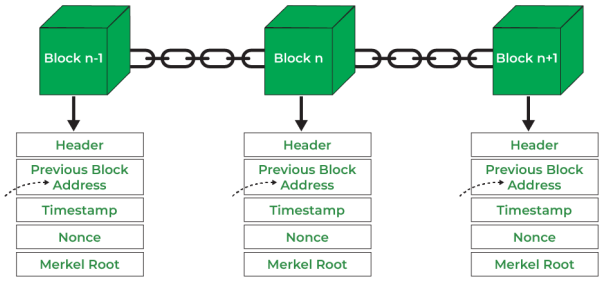

FIGURE 12. Blockchain structure.

B. PRIVATE BLOCKCHAIN

Compared to consortium blockchain and public blockchain, a private blockchain is likewise permissions and more centralized than a centralized one. Private blockchains are managed by a single organization responsible for determining who is allowed to join, carrying out consensus procedures, and keeping the shared ledger updated. Participants have a higher level of trust in private blockchains, and when compared to consortium blockchains, private blockchains function significantly better.

This type of chain, which is referred to as the permission chain, is often not accessible to the public and is utilized only by people or institutions [78]. Access to reading and writing on the private blockchain is regulated by regulations that private organizations have created. When it comes to data security, private chains place a high priority on preventing both internal and external threats, as well as providing users with a system that is transparent, tamper-proof, and safe. They offer a certain degree of centralized control rather than total decentralization, which means that they sacrifice some of the benefits that come with complete decentralization in exchange for superior performance in comparison to public chains.

A private blockchain is characterized as a permissioned network managed by a single organization, where access to transactions is restricted solely to individuals authorized to view them. Therefore, private blockchain offers a higher level of information privacy compared to public blockchain (Blockchain). Validating transactions is the responsibility of miners, which are a select group of nodes that engage in the cryptocurrency mining industry. Certain individuals, such as workers of an organization, are the only ones permitted to join the blockchain. In most cases, the process of creating blocks and reaching consensus is straightforward and quick. Because of the instantaneous finality of transactions, private blockchains can execute a huge number of transactions per second, even though they only permit a restricted number of nodes. Due to the small number of miners or nodes responsible for maintaining the network, the private blockchain is

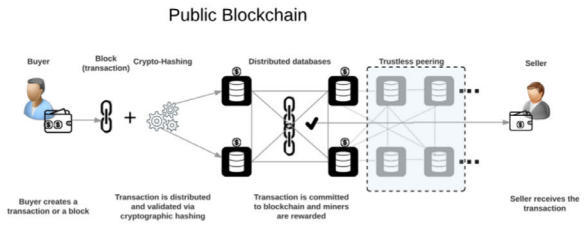

FIGURE 13. Public blockchain mode.

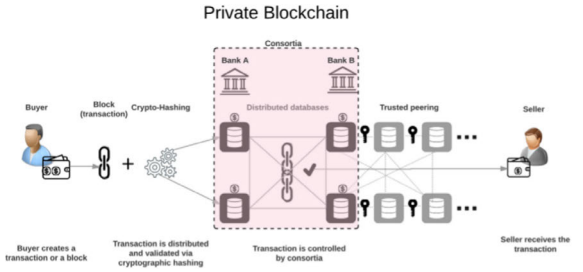

FIGURE 14. Private blockchain model.

considered somewhat centralized. This is because the fact that there are fewer miners or nodes increases the likelihood that the blockchain record will be altered. The private blockchains Hyperledger and Multichain are two instances of such blockchains.

C. CONSORTIUM BLOCKCHAIN

The consortium blockchain, also known as the hybrid blockchain, is an additional form of permissioned network between the public and private blockchain models. Within a consortium blockchain, a collection of organizations is in charge of regulating the access and permissions of nodes to the network, as well as the ability of those nodes to make modifications. This makes it possible for the node to carry out upgrades. A certain number of nodes are responsible for reaching a consensus in a consortium blockchain structure. While maintaining the benefits of the public blockchain, it restricts participation to just those who have been granted permission. On the other hand, it has a high throughput and greater speed than public blockchains, although it is less decentralized than public blockchains.

The consortium blockchain is a permissioned blockchain constructed by consortiums on behalf of many organizations. Considering that every organization constitutes a node on the blockchain, other organizations must obtain authorization from the consortium to join the consortium blockchain. Consortium blockchain is represented by Hyperledger Fabric, Corda, and Quorum, among other blockchain services. One of the corporate versions of Ethereum is called Quorum.

VI. BLOCKCHAIN KEY CHARACTERISTICS

Blockchain technologies have the following characteristics:

A. DECENTRALIZATION

Due to the blockchain's decentralized nature, authority is shared across all network nodes. Unlike the centralized system method, which depends on an authorized third party to function, this guarantees the redundancy of the system. The benefits of decentralization include increased trust, lower failure risk, and high service availability. The transaction validation process in conventional transaction management systems has been handled by a dependable organization (such as the government or a bank). At centralized service providers, this centralization approach invariably leads to additional costs, performance bottlenecks, and single-point failures (SPF). Blockchain, on the other hand, enables transactions to be verified between two peers without the need for central agency participation, authentication, or jurisdiction. This lowers the risk associated with SPF and lowers service costs while also decreasing performance bottlenecks and interference.

B. IMMUTABILITY

A permanent record of the transactions that are kept in the ledger is maintained and propagated throughout the nodes. Therefore, they cannot be changed in any way. Due to the unchangeable characteristics of blockchain technology, the ledger of blockchain is guaranteed to be accurate [79]. After they have been logged, the records in the ledger cannot be altered [80]. Any effort to modify the ledger entry for a specific block will result in the block being invalidated, and it will also weaken the dependability of the data throughout the whole blockchain. This is because the entire blockchain is a distributed ledger. Hashing and digital signatures are two examples of cryptographic procedures utilized to ensure the ledger is completely unchangeable. An in-depth examination of these methodologies is going to be provided in the essay. Modifying the ledger is a job that requires a significant amount of computer resources.

Every data block within a Blockchain is assigned a timestamp and encoded using a hash algorithm. This entered into the system is irreversible and cannot be altered until the majority of the nodes in the whole system reach a consensus [81], [82], and [83]. The transactions are publicly accessible and may be viewed by anybody at any moment. However, once verified and included in the Blockchain, such transactions become unchangeable and cannot be erased, making them irrevocable and immutable [84]. Any alteration, no matter how little, will create a fresh hash, which can be promptly detected, thereby ensuring the shared ledger remains uncorrupted [85]. This feature is quite useful when it comes to financial transactions and audits since it demonstrates that the data it contains has not been altered, regardless of whether it is being provided by the supplier or received by the recipient.

C. SECURITY

Blockchain is a decentralized distributed ledger technology, which means that any dishonest party wanting to change the blocks must first change the data recorded in all of the nodes that make up the network. Additional security measures

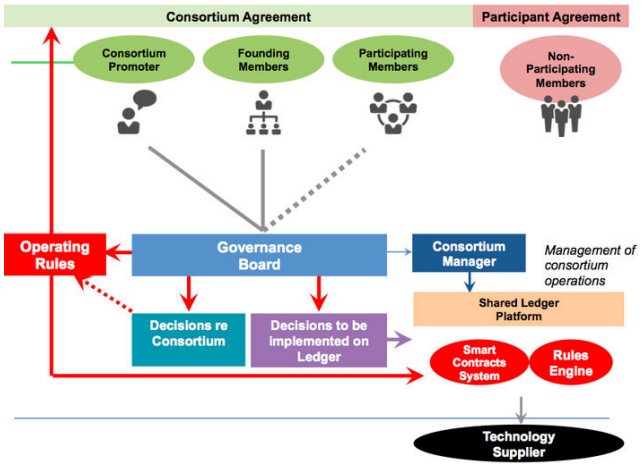

FIGURE 15. Consortium blockchain works.

are implemented through the utilization of encryption techniques, and the cryptographic hash is also utilized inside the blockchains [86].

Blockchain systems are intrinsically secure due to their use of asymmetrical cryptography. This involves a collection of common keys that are visible to all users and secret keys that are only visible to the system owner. Both [82] and [87] state These keys are used to verify whoever owns the transaction and ensure that the transaction remains unaltered. In the Blockchain system, security is associated with the integrity of transactions, the secrecy of transactions, and the permission of transactions [85]. The distributed nature of the Blockchain system, which also requires a P2P consensus mechanism, eliminates the possibility of a single point of failure for data. This is in contrast to data held centrally, which is far more susceptible to being compromised.

D. TRANSPARENT

Anyone may access the detailed information and historical records of every transaction recorded on the Blockchain database, ensuring complete transparency of transactions. Blockchain technology ensures a high degree of accountability and transparency for information, effectively prohibiting any unjust exploitation, untrustworthy additions, or withdrawals. Only Blockchain technology offers this degree of transparency. This level of openness is unmatched, especially for large financial organizations, and it represents a big advancement. The Blockchain system's transparency is facilitated by several verifying peer nodes that operate independently from a centralized authority [83]. Furthermore, the assets and transactions associated with each public address are readily available and visible to the public [85], leading to records of transactions that are easily traceable and characterized by transparency. In their study, Xinyi et al. [82] referred to the same notion using the word openness. Xinyi et al. state that the technical basis of Blockchain is freely available. Consequently, each node has the capability to create its own suitable apps by utilizing an accessible interface to retrieve information from the Blockchain. Consequently, both the data content and the operational regulations of the complete system are extensively accessible and clear, with no deceit occurring among the nodes [81]. The ideals of openness also extend to any alterations made to data recorded inside the Blockchain.

For several researchers, like Zheng et al. [88] and Ferrag et al. [87], the term ''auditability'' has been employed to denote the characteristics of transactions that are easily observable, straightforward to trace, and capable of being verified. Transparency has also been shown to be essential in the realm of healthcare and the disclosure of data from clinical studies. This trait is highly relevant for the financial accountability of huge businesses. Patients may employ the use of Blockchain in the healthcare sector to easily access and review their prior claims, medical records, transactions, and outstanding payments. Traditionally, the information gathered from clinical trials has not been shared with investigators medical professionals, and patients, resulting in a lack of trust and certainty in the findings [89]. Suggestions have been made regarding the use of blockchain-based approaches in order to track down the presence of documents that include pre-specified endpoints in clinical trials [90]. Furthermore, the utilization of smart contracts was suggested as a trusted administrator for the purpose of addressing data tampering difficulties that are frequently encountered in clinical studies [89]. The transparency inherent in Blockchain technology has been proven to be advantageous in tackling supply chain management misconduct and the lack of visibility in product history [91], [92], and [93].

Increasing the level of trust that voters have in the electoral process and ensuring that public elections are conducted without any fraud are two potential benefits of the transparency feature [94].

VII. THE NEEDS OF BLOCKCHAIN INTEGRATION WITH IoT

Through the Internet of Things (IoT), physical processes are being optimized and transformed in order to be transformed into aspects of the digital era. Huge amounts of information are being generated due to this process, resulting in the acquisition of knowledintge and insights on an unprecedented scale. This information contributes to the enhancement of residents' quality of life by facilitating the digitization of facilities across all key industries. According to Muñoz et al. [95], the installation of the Internet of Things (IoT) linked with cloud computing has shown to be quite beneficial. Similarly, blockchain technology can completely transform the existing structure of the Internet of Things (IoT), and the combination of the two would be extremely beneficial. A trustworthy information-sharing service that allows for the perceptibility and trustworthiness of data may be provided via blockchain technology. Due to the fact that the data is unchangeable and the origin of the data can be traced at any moment, the level of security automatically increases [96].

A. SECURITY ENHANCEMENT

A vast quantity of data is gathered from Internet of Things devices, and this data has to be protected by employing Blockchain technology since it can protect the data via encryption and cryptography techniques. Furthermore, the combination of Blockchain technology and the Internet of Things makes it possible to automatically update software in Internet of Things devices without compromising the confidentiality and safety of the data stored in those systems. As a result of the integration's ability to guarantee security, the danger of security breaches is reduced, and the Internet of Things system's resistance to attack is therefore strengthened [97]. According to Pan et al. [98], blockchains have the potential to safeguard the data that is produced by Internet of Things devices. This is because the data will be kept in the form of transactions that are encrypted and cryptographically signed. Furthermore, according to Zhang and Chen [99], incorporating blockchain technology resulted in the provision of automated software updates in Internet of Things devices. These updates proved to be an effective treatment for susceptible security breaches, improving the whole system's resilience.

The paper referenced proposes a groundbreaking binary spring search (BSS) method that integrates an adaptive deep neural network model [100]. This approach is based on group theory (GT). Detecting unauthorized intrusions into Internet of Things (IoT) systems is the goal of a privacy preservation strategy based on Blockchain technology.

In cryptography applications, protecting patient information is essential to guarantee the safety of the Internet of Medical Things (IoMT). The suggested approach enables consumers to protect information about patients and send it to the distributed database autonomously, without dependence on Blockchain administration. In [101], an innovative and disruptive encryption system that utilizes the structure of the Internet of Things. Blockchain is utilized to enhance the security and confidentiality of data originating from the Internet of Things.

Honsny H. et al. proposed a model that suggests combining blockchain technology with the LEACH (Low Energy Adaptive Clustering Herarchy) algorithm to improve the security of IoT networks. IoT devices clusters are created using the LEACH method, and each cluster is led by a cluster head (CH) who oversees data forwarding and aggregation. The LEACH algorithm extends the life of the network by distributing the energy burden evenly across devices through randomized rotations of CHs. They incorporated the fundamental ideas and cryptographic underpinnings of blockchain technology into the proposed model. The system architecture was shown in Figure 16. As a result, the network lifespan of the suggested model has significantly improved, and the energy resources used by sensor nodes increased which make it a viable method for extending the lifespan of IoT networks [102].

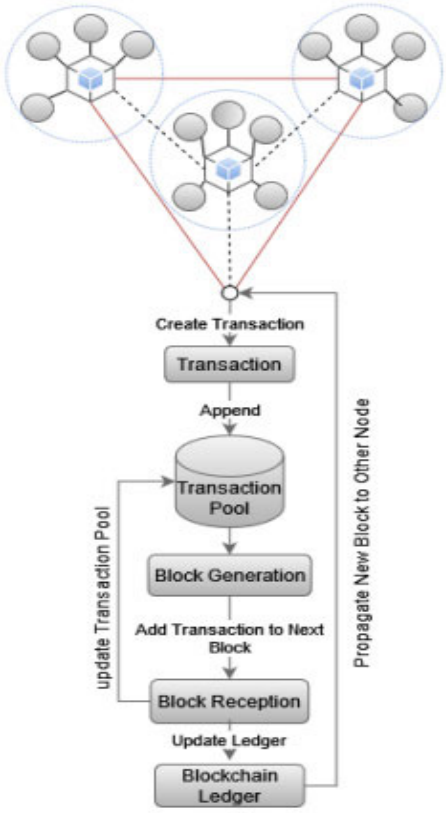

FIGURE 16. Proposed model system architecture.

B. INTEROPERABILITY

Enhancements should be made to enhance the interoperability of Internet of Things systems. Interoperability pertains to the ability of Internet of Things (IoT) systems to communicate with and exchange data among physical systems and other IoT systems. Blockchain technology can enhance the interoperability of Internet of Things, or IoT, systems by transforming and securely storing data from IoT devices in blocks. Blockchain technology has the potential to enhance interoperability in Internet of Things (IoT) networks by securely storing consumer and transaction data in a distributed ledger. The decentralized Blockchain platform facilitates converting, manipulating, extracting, and altering various types of Internets of Things (IoT) data. Additionally, it facilitates the creation of encrypted connections over different platforms or apps [97]. The study described in [103] presented a meticulously developed Blockchain platform that aims to bolster the dependability of IoT data and streamline compatibility across various Blockchain platforms. A distributed Blockchain-of-Blockchains (BoBs) is employed to guarantee concurrent integrity and compatibility. The proposed solution is built using Hyperledger Fabric and Ethermint to assess the viability of this idea. This technique converts, compresses, and stores the diverse data from the Internet of Things in a unified blockchain. As a result, it enables reliable access to different Internet of Things

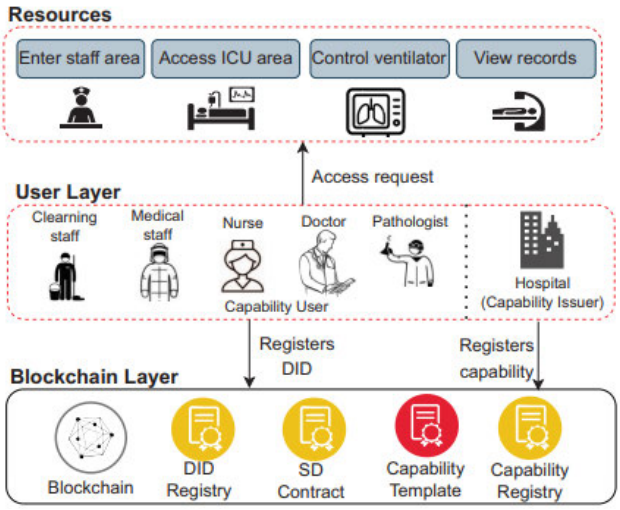

FIGURE 17. Blockchain-based interoperable access control.

systems interconnected as peers in the blockchain [99]. Blockchain technology has the capacity to enhance the interoperability of Internet of Things (IoT) systems by securely storing and modifying data produced by IoT devices within blockchains. Different types of Internets of Things datasets undergo modification, processing, mining, and resizing before being ultimately stored in the decentralized distributed ledger ecosystem.

R Mukta et al. suggested and designed a blockchain based access control architecture which uses a blockchain-based SSI ecosystem to enable selective information disclosure include identification and access control, with the goal of enhancing privacy-aware access management on Internet of Things (IoT) resources. The proposed architecture was shown in Figure 17. Redactable signatures are used in their proposed selective disclosure scheme to enable the creation of the ability to assert access rights on various resources while maintaining privacy. Additionally, by keeping only the capability's hash and the corresponding signature on the hash, their solution increased the efficiency of on-chain storage. By putting the suggested plan into practice and creating a Proof of Concept (PoC) prototype on the Hyperledger Blockchain, they assessed the viability and effectiveness. With a thorough performance study of the system's essential elements in terms of execution time, throughput, latency, and round-trip time, the trial findings demonstrated the system's viability [104].

C. DEPLOYMENT OF SOURCE CODE

Utilizing the immutable attributes of Blockchain can boost the secure and reliable implementation of software for IoT devices. This attribute enables the secure installation of programs from diverse origins within the IoT system [105]. On account of the fact that blockchain technology offers immutable and secure storage for transactions, it enables the safe deployment of codes into Internet of Things devices [106]. Additionally, it is possible to check the condition of Internet of Things devices and execute upgrades securely [107].

D. RELIABILITY

There is a widespread consensus that blockchain technology is highly reliable. Reliability is crucial in Blockchain-Internet of Things applications because it verifies the distributed network's effectiveness in ensuring the integrity of information and preventing any unauthorized alterations to the data. The integration of Blockchain with the Internet of Things framework ensures reliability and the availability and transparency of data acquired by Internet of Things sensors. The information stored in blockchain-based systems is immutable over time and remains dispersed over the whole network. As a result, the system members can authenticate the data and have the assurance that the data is not being tampered with. Blockchain technology also has the potential to enable accountability and traceability for sensor data.

When applied to the Internet of Things (IoT) paradigm, blockchain technology eliminates the requirement for centralized servers, which results in an increase in both information privacy and security. Utilizing the technology of blockchain in conjunction with Internet of Things technologies would result in the creation of a system that is both strong and resilient. Although it is common knowledge that the Internet of Things (IoT) can make the digitization of information easier, there is still a problem with the dependability of such information [107]. Blockchain technology resolved this issue by enhancing the dependability of a developed integrated system. A high level of resilience is ensured by the trustworthiness of blockchain technology, in addition to the extensive experience of its successful deployment in a variety of industries [108].

E. SERVICE MARKET

The use of blockchain technology has the capacity to accelerate the growth of an Internet of Things (IoT) system of information and service markets. This system will allow for the installation of microservices with ease and the processing of micropayments in a foolproof environment. Blockchain technology will make it possible for peers to conduct transactions without the need for central authorities.

Through a service market, transactions may occur between various companies without the need for any centralized body to monitor them. In addition to increasing the flexibility of Internet of Things systems in service markets, the independence of these systems also boosts the pace at which they execute. This not only permits secure communication in an environment that is completely foolproof, but it also makes it possible to deploy smaller services without increasing the amount of computing work that has to be done.

VIII. BLOCKCHAIN-BASED IoT APPLICATIONS

A lot of recent academic work has been done on blockchain-based Internet of Things, such as smart cities and associated smart surroundings. This section provides an overview of that study. The purpose of this part is to conduct an in-depth analysis of the most recent research advancements and organize them according to their possible

applications in blockchain-based smart cities. Multiple entities are accountable for upholding the decentralized record on a blockchain infrastructure inside an intelligent ecosystem. Smart contracts, in the meantime, are accountable for executing the operational rules and procedures of the firm.

A. SMART CITIES

Historically, the absence of a universally accepted standard for devices poses challenges in distributing data from diverse devices and creating compatibility across different functions. Biswas and Muthukkumarasamy [109] implemented a secure communication mechanism for smart cities utilizing blockchain technology. According to the authors, implementing blockchain in smart city nodes would create a distributed platform for secure device interaction. Additionally, blockchain technology prevents data integrity and availability assaults. Additionally, it offers an immutable transaction ledger for auditing purposes. Rahman et al. [110] developed a safe architecture for economic sharing in mega-smart cities using spatio-temporal smart contracts. In 2019, Yetis and Sahingoz [111] implemented a decentralized blockchain network structure utilizing blocks to establish a system for device authentication. Sabrina [112] proposed a method for managing access to resources in extensive Internet of Things (IoT) systems, such as those seen in smart cities. Public smart contracts and the blockchain are utilized for external access control, whilst local off-chain storage is employed for internal access control. In another study, Makhdoom et al. [113] introduced a blockchain architecture for smart city security.

Hakak et al. [114] introduced ''PrivySharing,'' a blockchain-based security architecture for safe IoT data exchange in smart cities. Blockchain is separated into channels with specialized data from a limited number of authorized organizations to ensure data privacy. Additionally, data in these channels is encrypted and collected privately to ensure security and isolation.

B. SMART HOMES

SHIB [115] is a smart house that utilizes IoT-Blockchain technology to address concerns such as scalability, secure connection supervision, and data confidentiality. The creator of ACC holds exclusive authority to add novel laws, modify current ones, or eliminate privacy limitations on the blockchain. To utilize the design, a cautious owner must have engaged in an intelligent contract with the correct individuals. Intelligent contracts may restrict access requests when there is network malfeasance, improving home data's security and privacy. This approach distinguishes itself from other current models by incorporating a Judge Contract (JC) with the authority to render decisions and enforce fines in response to misconduct. The ELIB [116] approach is designed to tackle unique obstacles linked to the application of blockchain technology and many challenges, including high bandwidth requirements, restricted scalability, and substantial computing complexity. The objective is to create an optimized smart home design that meets the requirements of the Internet of Things (IoT). Smart homes with limited resources might enhance their operations by employing a centrally managed manager that generates standardized keys for data transfer and manages all inbound and outbound requests. An overlay network is created using the ELIB paradigm, which enables the integration of sophisticated resources with a public blockchain to provide specialized safety and confidentiality features. The proposed ELIB model incorporates three optimizations: a Distributed Throughput Management (DTM) strategy, certificateless cryptography, and a streamlined consensus process. ELIB shows exceptional performance throughout the studies conducted using several criteria.

LSB [117] denotes a ''Lightweight Scalable Blockchain'' that employs network overlays to provide decentralized as well as full confidentiality. The clustering approach is employed to arrange network nodes into clusters, similar to the one outlined in the [118]. Throughout every pair of clusters, a Cluster Head (CH) is chosen to represent the node with the highest number of adjacent nodes. This is done to ensure optimal functionality of the cluster. CHs are designated to Overlay Block Managers (OBMs) since they are responsible for supervising the blockchain network. In Bitcoin, generating a genesis transaction necessitates using overlay nodes, which may be achieved by either the authority that issues certificates or the Burn coin technique. The beginning of a transaction is communicated between two OBM entities after undergoing verification. A system for consensus known as decentralized time-based was created to minimize latency and computing burden in the process of mining. The user's input is void of any content. Cluster leaders are responsible for efficiently applying the distributed trust mechanism across network nodes to authenticate new blocks. A distributed methodology is employed to manage network traffic effectively, ensuring its stability while taking into account unique characteristics. The main goal of LSB is to address the essential needs of the Internet of Things (IoT), including connection, adaptability, and real-time applications. It is utilized in many situations, including both high-end and low-end equipment. The authors conducted an analysis and subsequent discussion on many facets of LSB, including OBM reward, reliability, and complexity. LSB has demonstrated significant fault tolerance and resistance to various threats, as confirmed by a security evaluation. Additional assessment is necessary to ascertain the effectiveness of this notion in practical situations.

An authentication technique that ensures privacy is presented to demonstrate the process of collecting and sharing data in smart home apps [119]. The proposed method combines three key principles, namely intellectual edges, smart contracts, and attribute-based control of access, to produce a resilient and secure architecture. Data is securely and confidentially moved to the cloud via the use of a differential privacy approach. This approach alleviates the

computational load on systems, enhancing the system's adaptability. The proposed system architecture consists of clients, Internet of Things devices, multi-edge computers, and the cloud. Attribute-based access control employs two sorts of conventions: authorization contracts and access contracts. The authors thoroughly account for the transaction process, including four separate stages: linked transaction, status delivery, request administration, and initialization. The variation security enhancement approach consists of a fundamental method, hidden strategy, set of information, and implementation. The suggested method outperforms the present technique by offering enhanced security, privacy, resilience against assaults, precise access control, and reduced computational expenses.

C. HEALTHCARE

The smart city's main goal is to offer the general population cutting-edge healthcare services. The standards of care in a smart city refer to the degree of proficiency exhibited by healthcare services in achieving the intended medical results at individual as well as population levels [120]. The implementation of blockchain technology has the potential to significantly improve the healthcare business. The blockchain has the capability to keep complete electronic health records (EHR) by assigning a blockchain-based identity to each patient. To address difficulties related to information access, identity verification, and privacy, one can utilize smart contracts and access control technologies based on blockchain [121].

Effective coordination within the healthcare industry necessitates many entities having access to identical information on a patient's medical background, encompassing diagnosis and treatments. The decentralized nature of blockchain allows for the effective administration of data exchange and controlled accessibility amongst healthcare systems for therapeutic objectives. Moreover, blockchain technology may be utilized to oversee the entire medical product supply chain management process, including the travel of these items from manufacturing to distribution in pharmacy stores [122]. This application allows for identifying and preventing counterfeit medicines by scrutinizing the origin and history of medical products [123].

Azaria et al. [124] introduced a prototype called ''MedRec'' that utilizes blockchain technology to store electronic health data specifically for medical research purposes. MedRec offers a platform that allows for the immediate and seamless preservation of healthcare records, ensuring compatibility with other systems. Additionally, it places high importance on maintaining patient privacy and seeks to enhance the caliber and volume of data accessible for medical research. The distributed database system is firmly embedded in a similar fashion to the proof-of-work technique employed in Bitcoin. To ensure the integrity of the medical record, it is saved using its cryptographic hash, which effectively prevents any unauthorized alterations or tampering.

The authors in [125] examined the main challenges related to using a bitcoin-like open-source software blockchain for storing medical data. The primary issue is in the storage-intensive structure of healthcare data, which poses a hindrance to scaling up operations. Upon its production, a digital medical record is signed digitally by either the doctor who performed the surgery or the patient to authenticate its origin. The author suggests preserving just the utilization of searching meta-information, hash-pointers, and data encryption associated with the medical record on the public blockchain while keeping the entirety of the health information separate from the blockchain.

D. BUSINESS SUPPLY CHAIN

Businesses and industries require complicated supply chains where more than two organizations collaborate to control the flow of goods, services, money, and information from the source to the customer. This is called a supply chain. Individuals need a transparent, auditable, and secure supply chain system capable of encompassing comprehensive information, ranging from the origins of raw materials to the intricacies of the manufacturing process and from the production facility to the end consumer. The blockchain-powered supply chain solution ensures the secure storage of detailed information for each product in a single distributed ledger throughout its lifespan. The necessary information can be accessed by the right people.

In [91], Abeyratne and Monfared planned an industrial supply chain system ready for blockchain. They give every item a unique digital tag that lets them identify it. Everyone involved has been verified and can view the blockchain record. It was possible to enter data and look at the product description through a software tool. For each item in the supply chain, a smart contract is used to set the rules for handling it. Through a safe user interface, the ledger will provide proof beyond a doubt of who owns an object, as well as information on its position and time. The writers did not talk about the technical problems when blockchain is used in supply chain management, though.

In Alahmadi and Lin [126], suggested a fairness system for IIoT-based supply chain management built on blockchain. Technology safeguards the real-time exchange of tangible commodities among consumers and sellers by employing intelligent contracts to execute punitive measures and transmitting immutable transaction data over the blockchain. A new smart contract is set up for every trade deal, and the non-repudiation property is ensured by using a private key to digitally sign the transaction. Initialization, placing an order, delivery, and a judgement step by a smart contract are all parts of the trade process. The suggested plan was implemented with the EVM, and the performance was tested for the time it took for transactions to be confirmed in the blockchain network.

A study by Salah et al. [127] suggested using blockchain to make food and agriculture supply lines more efficient and effective at tracking things. Even though the study

was mostly about soybeans, the proposed plan can be used for any crop's agricultural supply chain (ASC). All parties involved used a blockchain platform to verify important factors like the country of origin, the current stage of crop processing, tracking yields, meeting quality standards, and following country-specific rules and regulations. All the people involved in the soybean agriculture supply chain (seed companies, farmers, grain elevators, grain processors, wholesalers, stores, and customers) had to follow the rules set by Ethereum-based smart contracts. However, the authors did not address the main problems in the farming supply chain, like handling disputes, making payments automatically, or stopping scams.

IX. CONCLUSION

The rapid increase in the usage of IoT has resulted in the introduction of several security vulnerabilities, encompassing attacks on both data and devices. The current IoT devices suffer from a lack of safety precautions and are unable to properly safeguard themselves largely because of their scarce resources, immature standards, poor compatibility, lack of protection in both software and hardware design, and problems in deployment and development. The scientific community has shown considerable interest in this, leading to numerous efforts to create a strong global foundation for IoT systems. In this ecosystem, using a decentralized and distributed technology called ''blockchain'' might offer solutions to security, privacy, traceability, reliability, and compatibility issues. The fundamental nature of blockchain technology ensures integrity, authenticity, and non-repudiation. Moreover, it facilitates the process of automating and validating transactions by utilizing smart contracts.

The article offers a concise account of the evolution of IoT and presents an extensive compilation of past attacks that have taken place in the IoT field. Next, please present a thorough and sophisticated analysis of blockchain technology, specifically emphasizing its characteristics and classification. In addition, the paper examines the possibilities of employing blockchain technology to tackle the most prominent security concerns on the Internet of Things. It also highlights the uses of blockchain technology in integrating various aspects of the Internet of Things. Hence, it can be deduced that the advancement and execution of Internet of Things technologies utilizing blockchain technology are currently in their nascent phases. In addition, additional technological advancements are required to meet the precise criteria for its wider adoption. Considering this, the study emphasizes many compelling avenues for further research that might be explored to improve the capability, scalability, and security of blockchains, anticipating a possible combination of blockchain technology with the Internet of Things.

REFERENCES

[1] Y. Sasaki, ''A survey on IoT big data analytic systems: Current and future,'' *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1024–1036, Jan. 2022, doi: 10.1109/JIOT.2021.3131724.

[2] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, ''A survey on security and privacy issues in Internet-of-Things,'' *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.

[3] Y. Lu and L. D. Xu, ''Internet of Things (IoT) cybersecurity research: A review of current research topics,'' *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019, doi: 10.1109/JIOT.2018.2869847.

[4] L. S. Angreani, A. Vijaya, and H. Wicaksono, ''Systematic literature review of Industry 4.0 maturity model for manufacturing and logistics sectors,'' *Proc. Manuf.*, vol. 52, pp. 337–343, Jan. 2020, doi: 10.1016/j.promfg.2020.11.056.

[5] Q.-D. Ngo, H.-T. Nguyen, V.-H. Le, and D.-H. Nguyen, ''A survey of IoT malware and detection methods based on static features,'' *ICT Exp.*, vol. 6, no. 4, pp. 280–286, Dec. 2020, doi: 10.1016/j.icte.2020.04.005.

[6] Y. Lu and X. Zheng, ''6G: A survey on technologies, scenarios, challenges, and the related issues,'' *J. Ind. Inf. Integr.*, vol. 19, Sep. 2020, Art. no. 100158, doi: 10.1016/j.jii.2020.100158.

[7] L. D. Xu, Y. Lu, and L. Li, ''Embedding blockchain technology into IoT for security: A survey,'' *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10452–10473, Jul. 2021, doi: 10.1109/JIOT.2021.3060508.

[8] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, ''A survey on blockchain technology: Evolution, architecture and security,'' *IEEE Access*, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

[9] K. Angrishi, ''Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV): IoT botnets,'' 2017, *arXiv:1702.03681*.

[10] M. Burhan, R. Rehman, B. Khan, and B.-S. Kim, ''IoT elements, layered architectures and security issues: A comprehensive survey,'' *Sensors*, vol. 18, no. 9, p. 2796, Aug. 2018, doi: 10.3390/s18092796.

[11] Bridgera. (2017). *IoT System, Sensors and Actuators*. [Online]. Available: https://bridgera.com/sensors-and-actuators-in-iot/

[12] Smarthomeblog. *How to Make Your Smoke Detecter Smarter*. [Online]. Available: https://smarthomeblog.net/smart-smoke-detector/

[13] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, ''Perception layer security in Internet of Things,'' *Future Gener. Comput. Syst.*, vol. 100, pp. 144–164, Nov. 2019, doi: 10.1016/j.future.2019.04.038.

[14] O. S. J. Nisha and S. M. S. Bhanu, ''A survey on code injection attacks in mobile cloud computing environment,'' in *Proc. 8th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Jan. 2018, pp. 1–6, doi: 10.1109/CONFLUENCE.2018.8443032.

[15] M. Devi and A. Majumder, ''Side-channel attack in Internet of Things: A survey,'' in *Applications of Internet of Things*, 2021, pp. 213–222, doi: 10.1007/978-981-15-6198-6_20.

[16] K. O. Adefemi Alimi, K. Ouahada, A. M. Abu-Mahfouz, and S. Rimer, ''A survey on the security of low power wide area networks: Threats, challenges, and potential solutions,'' *Sensors*, vol. 20, no. 20, p. 5800, Oct. 2020, doi: 10.3390/s20205800.

[17] C.-H. Liao, H.-H. Shuai, and L.-C. Wang, ''Eavesdropping prevention for heterogeneous Internet of Things systems,'' in *Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2018, pp. 1–2, doi: 10.1109/CCNC.2018.8319297.

[18] S. Abdelhamid, M. Aref, I. Hegazy, and M. Roushdy, ''A survey on learning-based intrusion detection systems for IoT networks,'' in *Proc. 10th Int. Conf. Intell. Comput. Inf. Syst. (ICICIS)*, Dec. 2021, pp. 278–288, doi: 10.1109/ICICIS52592.2021.9694226.

[19] 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. 82721–82743, 2019.

[20] N. Mishra and S. Pandya, ''Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review,'' *IEEE Access*, vol. 9, pp. 59353–59377, 2021, doi: 10.1109/ACCESS.2021.3073408.

[21] M. M. Ahemd, M. A. Shah, and A. Wahid, ''IoT security: A layered approach for attacks & defenses,'' in *Proc. Int. Conf. Commun. Technol. (ComTech)*, Apr. 2017, pp. 104–110, doi: 10.1109/COMTECH.2017.8065757.

[22] K. Zhao and L. Ge, ''A survey on the Internet of Things security,'' in *Proc. 9th Int. Conf. Comput. Intell. Secur.*, Dec. 2013, pp. 663–667, doi: 10.1109/CIS.2013.145.

[23] M. A. Khan and K. Salah, ''IoT security: Review, blockchain solutions, and open challenges,'' *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.

[24] G. Ikrissi and T. Mazri, "A study of smart campus environment and its security attacks," *Int. Arch. Photogramm., Remote Sens. Spatial Inf. Sci.*, vol. XLIV-4, pp. 255–261, Nov. 2020, doi: 10.5194/isprs-archives-xliv-4-w3-2020-255-2020.
[25] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, Mar. 2022, doi: 10.1002/ett.3677.
[26] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors*, vol. 20, no. 13, p. 3625, Jun. 2020, doi: 10.3390/s20133625.
[27] K. Nirmal, B. Janet, and R. Kumar, "Analyzing and eliminating phishing threats in IoT, network and other web applications using iterative intersection," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 4, pp. 2327–2339, Jul. 2021, doi: 10.1007/s12083-020-00944-z.
[28] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommun. Syst.*, vol. 73, no. 1, pp. 3–25, Jan. 2020, doi: 10.1007/s11235-019-00599-z.
[29] A. Raoof, A. Matrawy, and C.-H. Lung, "Enhancing routing security in IoT: Performance evaluation of RPL's secure mode under attacks," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11536–11546, Dec. 2020, doi: 10.1109/JIOT.2020.3022276.
[30] I. Hafeez, M. Antikainen, and S. Tarkoma, "Protecting IoT-environments against traffic analysis attacks with traffic morphing," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2019, pp. 196–201, doi: 10.1109/PERCOMW.2019.8730787.
[31] S. N. Swamy, D. Jadhav, and N. Kulkarni, "Security threats in the application layer in IoT applications," in *Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)*, Feb. 2017, pp. 477–480, doi: 10.1109/I-SMAC.2017.8058395.
[32] B. Prabadevi and N. Jeyanthi, "A review on various sniffing attacks and its mitigation techniques," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 12, no. 3, p. 1117, Dec. 2018, doi: 10.11591/ijeecs.v12.i3.pp1117-1125.
[33] A. Kamble, V. S. Malemath, and D. Patil, "Security attacks and secure routing protocols in RPL-based Internet of Things: Survey," in *Proc. Int. Conf. Emerg. Trends Innov. ICT (ICEI)*, Feb. 2017, pp. 33–39, doi: 10.1109/ETIICT.2017.7977006.
[34] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 644–653, May 2014, doi: 10.1016/j.jcss.2013.06.016.
[35] M. Goyal and M. Dutta, "Intrusion detection of wormhole attack in IoT: A review," in *Proc. Int. Conf. Circuits Syst. Digit. Enterprise Technol. (ICCSDET)*, Dec. 2018, pp. 1–5, doi: 10.1109/ICCSDET.2018.8821160.
[36] S. Rachmadi, S. Mandala, and D. Oktaria, "Detection of DoS attack using AdaBoost algorithm on IoT system," in *Proc. Int. Conf. Data Sci. Its Appl. (ICoDSA)*, Oct. 2021, pp. 28–33, doi: 10.1109/ICoDSA53588.2021.9617545.
[37] L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider, and G. Saldamli, "Predicting and preventing cyber attacks during COVID-19 time using data analysis and proposed secure IoT layered model," in *Proc. 4th Int. Conf. Multimedia Comput., Netw. Appl. (MCNA)*, Oct. 2020, pp. 113–118, doi: 10.1109/MCNA50957.2020.9264301.
[38] R. Arthi and S. Krishnaveni, "Design and development of IoT testbed with DDoS attack for cyber security research," in *Proc. 3rd Int. Conf. Signal Process. Commun. (ICPSC)*, May 2021, pp. 586–590, doi: 10.1109/ICSPC51351.2021.9451786.
[39] 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, doi: 10.1109/MC.2017.201.
[40] R. P. Kumar and S. Smys, "A novel report on architecture, protocols and applications in Internet of Things (IoT)," in *Proc. 2nd Int. Conf. Inventive Syst. Control (ICISC)*, Jan. 2018, pp. 1156–1161, doi: 10.1109/ICISC.2018.8398986.
[41] D. Dinculeană and X. Cheng, "Vulnerabilities and limitations of MQTT protocol used between IoT devices," *Appl. Sci.*, vol. 9, no. 5, p. 848, Feb. 2019, doi: 10.3390/app9050848.
[42] H. Akram, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, pp. 355–373, 2018, doi: 10.14569/ijacsa.2018.090349.
[43] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in Internet of Things: Challenges, solutions and future directions," in *Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2016, pp. 5772–5781, doi: 10.1109/HICSS.2016.714.
[44] Q. Zhang and X. Wang, "SQL injections through back-end of RFID system," in *Proc. Int. Symp. Comput. Netw. Multimedia Technol.*, Jan. 2009, pp. 1–4, doi: 10.1109/CNMT.2009.5374533.
[45] Z. X. Yang, "SQL injection-database attack revolution and prevention," *Appl. Mech. Mater.*, vol. 740, pp. 810–814, Mar. 2015, doi: 10.4028/www.scientific.net/amm.740.810.
[46] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the Internet of Things (IoT): A security taxonomy for IoT," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.,12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 163–168, doi: 10.1109/TrustCom/BIGDATASE.2018.00034.
[47] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Gener. Comput. Syst.*, vol. 108, pp. 909–920, Jul. 2020, doi: 10.1016/j.future.2018.04.027.
[48] B. Ahlawat, A. Sangwan, and V. Sindhu, "IoT system model, challenges and threats," *Int. J. Sci. Technol. Res.*, vol. 9, no. 3, pp. 6771–6776, 2020.
[49] M. Waqas, K. Kumar, A. A. Laghari, U. Saeed, M. M. Rind, A. A. Shaikh, F. Hussain, A. Rai, and A. Q. Qazi, "Botnet attack detection in Internet of Things devices over cloud environment via machine learning," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 4, p. 6662, Feb. 2022, doi: 10.1002/cpe.6662.
[50] F. Hussain, S. G. Abbas, I. M. Pires, S. Tanveer, U. U. Fayyaz, N. M. Garcia, G. A. Shah, and F. Shahzad, "A two-fold machine learning approach to prevent and detect IoT botnet attacks," *IEEE Access*, vol. 9, pp. 163412–163430, 2021, doi: 10.1109/ACCESS.2021.3131014.
[51] F. Hussain, S. G. Abbas, U. U. Fayyaz, G. A. Shah, A. Toqeer, and A. Ali, "Towards a universal features set for IoT botnet attacks detection," in *Proc. IEEE 23rd Int. Multitopic Conf. (INMIC)*, Nov. 2020, pp. 1–6, doi: 10.1109/INMIC50486.2020.9318106.
[52] N. Vlajic and D. Zhou, "IoT as a land of opportunity for DDoS hackers," *Computer*, vol. 51, no. 7, pp. 26–34, Jul. 2018, doi: 10.1109/MC.2018.3011046.
[53] N. Sivasankari and S. Kamalakkannan, "Detection and prevention of man-in-the-middle attack in IoT network using regression modeling," *Adv. Eng. Softw.*, vol. 169, Jul. 2022, Art. no. 103126, doi: 10.1016/j.advengsoft.2022.103126.
[54] E. Ylli and J. Fejzaj, "Man in the middle: Attack and protection," *CEUR Workshop Proc.*, vol. 2872, no. May, pp. 198–204, May 2021.
[55] A. A. Tadesse, "A thesis prepared by: Abel Ashenafi Tadesse," Tech. Rep., 2022.
[56] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. B. Dhaou, "Distributed denial of service attack detection for the Internet of Things using hybrid deep learning model," *IEEE Access*, vol. 11, pp. 119862–119875, 2023, doi: 10.1109/ACCESS.2023.3327620.
[57] X. Chen, L. Xiao, W. Feng, N. Ge, and X. Wang, "DDoS defense for IoT: A Stackelberg game model-enabled collaborative framework," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9659–9674, Jun. 2022, doi: 10.1109/JIOT.2021.3138094.
[58] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, "Internet of Things security: Challenges and key issues," *Secur. Commun. Netw.*, vol. 2021, pp. 1–11, Sep. 2021, doi: 10.1155/2021/5533843.
[59] W. I. Khedr, A. E. Gouda, and E. R. Mohamed, "FMDADM: A multilayer DDoS attack detection and mitigation framework using machine learning for stateful SDN-based IoT networks," *IEEE Access*, vol. 11, pp. 28934–28954, 2023, doi: 10.1109/ACCESS.2023.3260256.
[60] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, and H. Karimipour, "Secure intelligent fuzzy blockchain framework: Effective threat detection in IoT networks," *Comput. Ind.*, vol. 144, Jan. 2023, Art. no. 103801, doi: 10.1016/j.compind.2022.103801.
[61] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoudeh, H. Karimipour, and G. Srivastava, "Block hunter: Federated learning for cyber threat hunting in blockchain-based IIoT networks," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 8356–8366, Nov. 2022, doi: 10.1109/TII.2022.3168011.
[62] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K. R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1120–1132, Apr. 2021, doi: 10.1109/TNSE.2019.2937481.
[63] O. Mounnan, A. El Mouatasim, O. Manad, T. Hidar, A. A. El Kalam, and N. Idboufker, "Privacy-aware and authentication based on blockchain with fault tolerance for IoT enabled fog computing," in *Proc. 5th Int. Conf. Fog Mobile Edge Comput. (FMEC)*, Apr. 2020, pp. 347–352, doi: 10.1109/FMEC49853.2020.9144845.

[64] P. Khordadpour and S. Ahmadi, "Security and privacy enhancing in blockchain-based IoT environments via anonym auditing," 2024, *arXiv:2403.01356*.

[65] J. Ali, T. Ali, Y. Alsaawy, A. S. Khalid, and S. Musa, "Blockchain-based smart-IoT trust zone measurement architecture," in *Proc. ACM Int. Conf. Omni-Layer Intell. Syst.*, Apr. 2019, no. April, pp. 152–157, doi: 10.1145/3312614.3312646.

[66] P. Patil, M. Sangeetha, and V. Bhaskar, "Blockchain for IoT access control, security and privacy: A review," *Wireless Pers. Commun.*, vol. 117, no. 3, pp. 1815–1834, Apr. 2021, doi: 10.1007/s11277-020-07947-2.

[67] B. W. Nyamtiga, J. C. S. Sicato, S. Rathore, Y. Sung, and J. H. Park, "Blockchain-based secure storage management with edge computing for IoT," *Electronics*, vol. 8, no. 8, p. 828, Jul. 2019, doi: 10.3390/electronics8080828.

[68] Q.-U.-A. Arshad, W. Z. Khan, F. Azam, M. K. Khan, H. Yu, and Y. B. Zikria, "Blockchain-based decentralized trust management in IoT: Systems, requirements and challenges," *Complex Intell. Syst.*, vol. 9, no. 6, pp. 6155–6176, Dec. 2023, doi: 10.1007/s40747-023-01058-8.

[69] A. Hughes, A. Park, J. Kietzmann, and C. Archer-Brown, "Beyond bitcoin: What blockchain and distributed ledger technologies mean for firms," *Bus. Horizons*, vol. 62, no. 3, pp. 273–281, May 2019, doi: 10.1016/j.bushor.2019.01.002.

[70] F. A. Abadi, J. Ellul, and G. Azzopardi, "The blockchain of things, beyond bitcoin: A systematic review," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1666–1672, doi: 10.1109/Cybermatics_2018.2018.00278.

[71] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019, doi: 10.1109/JIOT.2019.2920987.

[72] R. Ramadoss, "Blockchain technology: An overview," *IEEE Potentials*, vol. 41, no. 6, pp. 6–12, Nov. 2022, doi: 10.1109/MPOT.2022.3208395.

[73] V. Srivastava, A. Baksi, and S. K. Debnath, "An overview of hash based signatures," Cryptol. ePrint Arch., Tech. Rep., 2023.

[74] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," in *Proc. Int. Conf. Electron., Commun. Comput. Eng. (ICECCE)*, Nov. 2014, pp. 83–93, doi: 10.1109/ICECCE.2014.7086640.

[75] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm validation system (ECDSAVS)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Sep. 2001. [Online]. Available: http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf

[76] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu, "Survey: Sharding in blockchains," *IEEE Access*, vol. 8, pp. 14155–14181, 2020, doi: 10.1109/ACCESS.2020.2965147.

[77] C. Brunner, A. Madhusudan, D. Engel, and B. Preneel, "Off-chain state channels in the energy domain," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2021, pp. 1–5, doi: 10.1109/ISGT49243.2021.9372246.

[78] S. Thakur and V. Kulkarni, "Blockchain and its applications—A detailed survey," *Int. J. Comput. Appl.*, vol. 180, no. 3, pp. 29–35, Dec. 2017, doi: 10.5120/ijca2017915994.

[79] H. S. Kim and K. Wang, "Immutability measure for different blockchain structures," in *Proc. IEEE 39th Sarnoff Symp.*, Sep. 2018, pp. 1–6, doi: 10.1109/SARNOF.2018.8720496.

[80] F. Hofmann, S. Wurster, E. Ron, and M. Böhmecke-Schwafert, "The immutability concept of blockchains and benefits of early standardization," in *Proc. ITU Kaleidoscope, Challenges Data-Driven Soc. (ITU K)*, Nov. 2017, pp. 1–8, doi: 10.23919/ITU-WT.2017.8247004.

[81] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, Sep. 2017, doi: 10.6633/IJNS.201709.19(5).01.

[82] Y. Xinyi, Z. Yi, and Y. He, "Technical characteristics and model of blockchain," in *Proc. 10th Int. Conf. Commun. Softw. Netw. (ICCSN)*, Jul. 2018, pp. 562–566, doi: 10.1109/ICCSN.2018.8488289.

[83] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019, doi: 10.1109/COMST.2019.2894727.

[84] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consum. Electron. Mag.*, vol. 7, no. 2, pp. 18–21, Mar. 2018, doi: 10.1109/MCE.2017.2776459.

[85] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019, doi: 10.1109/COMST.2019.2899617.

[86] A. Draper, A. Familrouhani, D. Cao, T. Heng, and W. Han, "Security applications and challenges in blockchain," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2019, pp. 1–4, doi: 10.1109/ICCE.2019.8661914.

[87] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019, doi: 10.1109/JIOT.2018.2882794.

[88] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564, doi: 10.1109/BIGDATACONGRESS.2017.85.

[89] T. Nugent, D. Upton, and M. Cimpoesu, "Improving data transparency in clinical trials using blockchain smart contracts," *FResearch*, vol. 5, p. 2541, Oct. 2016, doi: 10.12688/f1000research.9756.1.

[90] G. Irving and J. Holden, "How blockchain-timestamped protocols could improve the trustworthiness of medical science," *FResearch*, vol. 5, p. 222, Mar. 2017, doi: 10.12688/f1000research.8114.3.

[91] S. A. A., "Blockchain ready manufacturing supply chain using distributed ledger," *Int. J. Res. Eng. Technol.*, vol. 5, no. 9, pp. 1–10, Sep. 2016.

[92] K. Francisco and D. Swanson, "The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency," *Logistics*, vol. 2, no. 1, p. 2, Jan. 2018, doi: 10.3390/logistics2010002.

[93] S. E. Chang and Y. Chen, "When blockchain meets supply chain: A systematic literature review on current development and potential applications," *IEEE Access*, vol. 8, pp. 62478–62494, 2020, doi: 10.1109/ACCESS.2020.2983601.

[94] T. Moura and A. Gomes, "Blockchain voting and its effects on election transparency and voter confidence," in *Proc. 18th Annu. Int. Conf. Digit. Government Res.*, Jun. 2017, pp. 574–575, doi: 10.1145/3085228.3085263.

[95] R. Muñoz, R. Vilalta, N. Yoshikane, R. Casellas, R. Martínez, T. Tsuritani, and I. Morita, "Integration of IoT, transport SDN, and edge/cloud computing for dynamic distribution of IoT analytics and efficient use of network resources," *J. Lightw. Technol.*, vol. 36, no. 7, pp. 1420–1428, Apr. 1, 2018, doi: 10.1109/JLT.2018.2800660.

[96] R. Sethi, B. Bhushan, N. Sharma, R. Kumar, and I. Kaushik, "Applicability of industrial IoT in diversified sectors: Evolution, applications and challenges," in *Multimedia Technologies in the Internet of Things Environment*, 2020, pp. 45–67, doi: 10.1007/978-981-15-7965-3_4.

[97] D. Miraz and M. Ali, "Integration of blockchain and IoT: An enhanced security perspective," 2020, *arXiv:2011.09121*.

[98] W. Pan, F. Zheng, Y. Zhao, W.-T. Zhu, and J. Jing, "An efficient elliptic curve cryptography signature server with GPU acceleration," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 111–122, Jan. 2017, doi: 10.1109/TIFS.2016.2603974.

[99] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58241–58254, 2019, doi: 10.1109/ACCESS.2018.2890736.

[100] A. Ali, M. A. Almaiah, F. Hajjej, M. F. Pasha, O. H. Fang, R. Khan, J. Teo, and M. Zakarya, "An industrial IoT-based blockchain-enabled secure searchable neural network," *Sensors*, vol. 22, no. 2, p. 572, 2022.

[101] R. Durga, E. Poovammal, K. Ramana, R. H. Jhaveri, S. Singh, and B. Yoon, "CES blocks—A novel chaotic encryption schemes-based blockchain system for an IoT environment," *IEEE Access*, vol. 10, pp. 11354–11371, 2022, doi: 10.1109/ACCESS.2022.3144681.

[102] H. H. A. Emira, A. A. Elngar, and M. Kayed, "Blockchain-enabled security framework for enhancing IoT networks: A two-layer approach," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 10, pp. 550–561, 2023, doi: 10.14569/ijacsa.2023.0141059.

[103] M. S. Rahman, M. A. P. Chamikara, I. Khalil, and A. Bouras, "Blockchain-of-blockchains: An interoperable blockchain platform for ensuring IoT data integrity in smart city," *J. Ind. Inf. Integr.*, vol. 30, Nov. 2022, Art. no. 100408, doi: 10.1016/j.jii.2022.100408.

[104] R. Mukta, S. Pal, S. Mishra, H.-Y. Paik, S. S. Kanhere, and M. Hitchens, "A blockchain-based interoperable architecture for IoT with selective disclosure of information," in *Proc. IEEE 28th Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Oct. 2023, pp. 53–63, doi: 10.1109/PRDC59308.2023.00016.

[105] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based efficient and incentive approach," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6367–6378, Dec. 2019, doi: 10.1109/TII.2019.2917307.

[106] M. Samaniego and R. Deters, "Hosting virtual IoT resources on edge-hosts with blockchain," in *Proc. IEEE Int. Conf. Comput. Inf. Technol. (CIT)*, Dec. 2016, pp. 116–119, doi: 10.1109/CIT.2016.71.

[107] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018, doi: 10.1016/j.future.2018.05.046.

[108] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Proc. Comput. Sci.*, vol. 132, pp. 1815–1823, Jan. 2018, doi: 10.1016/j.procs.2018.05.140.

[109] T. M. Ghazal, M. K. Hasan, H. M. Alzoubi, M. Al Hmmadi, N. A. Al-Dmour, S. Islam, R. Kamran, and B. Mago, "Securing smart cities using blockchain technology," in *Proc. 1st Int. Conf. AI Cybersecurity (ICAIC)*, May 2022, pp. 1–4, doi: 10.1109/ICAIC53980.2022.9896971.

[110] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18611–18621, 2019, doi: 10.1109/ACCESS.2019.2896065.

[111] R. Yetis and O. K. Sahingoz, "Blockchain based secure communication for IoT devices in smart cities," in *Proc. 7th Int. Istanbul Smart Grids Cities Congr. Fair (ICSG)*, Apr. 2019, pp. 134–138, doi: 10.1109/SGCF.2019.8782285.

[112] F. Sabrina, "Blockchain and structural relationship based access control for IoT: A smart city use case," in *Proc. IEEE 44th Conf. Local Comput. Netw. (LCN)*, Oct. 2019, pp. 137–140, doi: 10.1109/LCN44214.2019.8990757.

[113] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1636–1675, 2nd Quart., 2019, doi: 10.1109/COMST.2018.2874978.

[114] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani, "Securing smart cities through blockchain technology: Architecture, requirements, and challenges," *IEEE Netw.*, vol. 34, no. 1, pp. 8–14, Jan. 2020, doi: 10.1109/MNET.001.1900178.

[115] T. L. N. Dang and M. S. Nguyen, "An approach to data privacy in smart home using blockchain technology," in *Proc. Int. Conf. Adv. Comput. Appl. (ACOMP)*, Nov. 2018, pp. 58–64, doi: 10.1109/ACOMP.2018.00017.

[116] S. N. Mohanty, K. C. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. K. Lakshmanaprabu, and A. Khanna, "An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy," *Future Gener. Comput. Syst.*, vol. 102, pp. 1027–1037, Jan. 2020, doi: 10.1016/j.future.2019.09.050.

[117] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and anonymity," *J. Parallel Distrib. Comput.*, vol. 134, pp. 180–197, Dec. 2019, doi: 10.1016/j.jpdc.2019.08.005.

[118] A. Kousaridas, S. Falangitis, P. Magdalinos, N. Alonistioti, and M. Dillinger, "SYSTAS: Density-based algorithm for clusters discovery in wireless networks," in *Proc. IEEE 26th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Aug. 2015, pp. 2126–2131, doi: 10.1109/PIMRC.2015.7343649.

[119] A. Qashlan, P. Nanda, X. He, and M. Mohanty, "Privacy-preserving mechanism in smart home using blockchain," *IEEE Access*, vol. 9, pp. 103651–103669, 2021, doi: 10.1109/ACCESS.2021.3098795.

[120] W. Glover, Q. Li, E. Naveh, and M. Gross, "Improving quality of care through integration in a hospital setting: A human systems integration approach," *IEEE Trans. Eng. Manag.*, vol. 64, no. 3, pp. 365–376, Aug. 2017, doi: 10.1109/TEM.2017.2682267.

[121] G. Ali, N. Ahmad, Y. Cao, Q. E. Ali, F. Azim, and H. Cruickshank, "BCON: Blockchain based access CONtrol across multiple conflict of interest domains," *J. Netw. Comput. Appl.*, vol. 147, Dec. 2019, Art. no. 102440, doi: 10.1016/j.jnca.2019.102440.

[122] S. Angraal, H. M. Krumholz, and W. L. Schulz, "Blockchain technology: Applications in health care," *Circulat., Cardiovascular Quality Outcomes*, vol. 10, no. 9, pp. 1–3, Sep. 2017, doi: 10.1161/circoutcomes.117.003800.

[123] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Sep. 2016, pp. 1–3, doi: 10.1109/HEALTHCOM.2016.7749510.

[124] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.

[125] L. A. Linn and M. B. Koo, "A blockchain for health care," Tech. Rep., 2014, pp. 1–10.

[126] A. Alahmadi and X. Lin, "Towards secure and fair IIoT-enabled supply chain management via blockchain-based smart contracts," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–7, doi: 10.1109/ICC.2019.8761216.

[127] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain-based soybean traceability in agricultural supply chain," *IEEE Access*, vol. 7, pp. 73295–73305, 2019, doi: 10.1109/ACCESS.2019.2918000.

NATHALIE TAN YHE HUAN (Member, IEEE) received the bachelor's degree (Hons.) in electronic engineering technology (communication and computer) from Universiti Tun Hussein Onn Malaysia, Johor, Malaysia, in 2023. She is currently pursuing the master's degree in computer networks with University Putra Malaysia, Selangor, Malaysia.

ZURIATI AHMAD ZUKARNAIN (Member, IEEE) received the B.S. and M.S. degrees in physics and education from University Putra Malaysia (UPM), Selangor, Malaysia, in 1997 and 2000, respectively, and the Ph.D. degree in quantum computing and communication from the University of Bradford, U.K., in 2005. She has been an Academic Staff with the Faculty of Computer Science and Information Technology, UPM, since 2001. She was the Head of the Department of Communication Technology and Networks, from 2006 to 2011. She was also the Head of the Section of High-Performance Computing, Institute of Mathematical Research, UPM, from 2012 to 2015. She taught several courses for undergraduate students, such as data communication and networks, distributed systems, mobile and wireless, network security, computer architecture, and assembly language. She taught a few courses for postgraduate students, such as the advanced distributed and research method. Her current research interests include computer networks, distributed systems, mobile and wireless, network security, quantum computing, and quantum cryptography. She is a member of the IEEE Computer Society.