Mitigating Security and Privacy issues in IoT Application using Blockchain: A Review

P.Shorubiga,
Department of Physical Science,
Faculty of Applied Science,
University of Vavuniya
pshorubiga@vau.ac.lk

R.Shyam,
Department of ICT,
Faculty of Technological Studies,
University of Vavuniya
shyam2ravi@gmail.com

***Abstract*— We live in a world where everything is connected via the Internet of Things (IoT). Despite this, IoT privacy remains a serious challenge, particularly due to IoT networks' vast scale and dispersed nature. Using protected solutions, such as incorporating blockchain technology into privacy-based services, is one approach to privacy-related concerns. Various Internet of Things security and authentication issues have been resolved by the decentralized nature of blockchain technology. This paper examines how blockchain technology mitigates the security and privacy concerns of IoT networks. In addition, we investigate the structure and uses of blockchain technology for recommender system privacy and trust management solutions. The limitations of adopting the blockchain technology also discussed. From the analysis of literature works, the blockchain technology could be able to circumvent IoT limitations such as data security and privacy. In addition, it may offer IoT customers distributed storage, transparency, trust, safe distributed IoT networks, and privacy and security assurance.**

Keywords*— Blockchain, Internet of Things (IoT), privacy, security, Literature review, cyber security

I. Introduction

The Internet of Things (IoT) is the fastest-growing technology of the previous decade, as the use of smart gadgets and accompanying apps has exploded in both industry and science [1]. The massive increase in IoT device adoption may be ascribed to two factors: lower computing costs and widespread availability of wireless connectivity [2]. It is made up of a variety of sensor-embedded devices that can communicate with one another without the need for human intervention [3]. These things will be able to link and interact with one other and with their environment simplifying many of our actions. The Internet of Things (IoT) comprises numerous present and future interoperable, networked information and communication technology (ICT) systems, as well as additional artifacts and services. Healthcare, industry, the internet of things (IoT), aviation, travel & hospitality (including wearables), and more are all incorporating IoT. While the Internet of Things presents manufacturing opportunities, it nonetheless creates significant challenges. Because present encryption and cryptography methods are insufficient, smart objects are vulnerable to assaults due to a lack of storage space and computational power [4]. As a result, security and privacy have been major issues that will not be overlooked as the Internet of Things grows. However, as the number of IoT devices grows at an exponential rate, preserving the crucial data generated by these devices has become a major challenge. As a result, Critical IoT data were kept with a third cloud platform provider in the cloud based IoT infrastructure standard [5]. However, because the cloud server has access to all the data included in the private IoT data, the cloud server can divulge it. Despite this, blockchain storage is seen as a distributed and decentralized archiving system [5]. Things and systems in IoT might be compelled to communicate with a central server for authentication because of their dynamic connectivity, network interconnectedness, and scattered existence. Distributed and decentralized, blockchain storage is a mechanism for storing data. Data is exchanged and maintained on hundreds of nodes throughout the world via peer-to-peer networks, with repeated algorithms creating more copies.

As such, this study will conduct a Systematic Literature Review (SLR) to assess how security and privacy measures have been applied to it. Specifically, this article concentrated on four-fold.

- A paper analyzing present Blockchain functionality concerns and challenges across multiple categories.

- A summary of the Blockchain architectures that have been considered and implemented in the literature.

- A privacy-focused assessment of Blockchain technology, considering both security and privacy concerns.

- A study of the privacy implications of Blockchain technology in applications that might act as a framework for continued research.

The remainder of this research discusses similar literature assessments on Blockchain for security in addition to the analysis's significant results and findings.

II. Method

This section discusses the technique followed to do the study, including the research questions, eligibility conditions, information sources and search, study selection, and data gathering. This article uses "ELSEVIER" AND "IEEE Xplore" as its main study resources, with "Blockchain", “IoT” and "Privacy Security" OR "Security" as its key search terms.

- It should be a full-length paper or journal article, as these are fully peer-reviewed and always contain pertinent study material.

- It must focus on security measures adopted in IoT and Blockchain.

- It must strive to fix or raise security and privacy problems.

This review followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) statement [6] and was supplemented with Kitchenham's standard criteria to [7] satisfy this area.

It identified relevant research papers in a total of 156 and checked for duplicates in the other database. Between these datasets, no duplicates were discovered. The database is then filtered depending on eligibility criteria, resulting in a total of 50 records. The next step is to filter based on the content, which must be a full-text article or journal article that entirely addresses the aim and has been suitably peer-reviewed. Given the research question, it is now time to choose 23 papers for the final qualitative synthesis, which will contain survey data.

III. Internet of Things

The Internet's evolution began with the connection of computers. Later, more computers were linked, creating the World Wide Web. The development of mobile-Internet technology was sparked by the capacity of mobile devices to connect to the Internet. People began to utilize the internet through social networks. Eventually, the concept of linking everyday things to the internet was introduced, causing the growth of the Internet of Things technology [6]. IoT architecture is typically categorized into four tiers.

A. Perception Layer

At this level of the IoT Architecture, sensors, embedded systems (e.g., RFID tags and readers), and other soft sensors are implemented in the field. Each of these sensors includes capabilities such as identification and data storage (for example, RFID tags), data collection (– for example, sensor networks), and far more [2].

B. Network Layer and Access Gateway

This layer is responsible for transmitting data gathered via sensors to the subsequent layer. It should be able to provide a worldwide protocol for data transmission across heterogeneous systems that is scalable, adaptable, and standards based. This layer should be responsive and have a robust network. Additionally, it should enable autonomous communication between multiple groups.

C. Transport Layer

This layer establishes a bidirectional connection between the network and application layers. It is responsible for the administration of equipment and information, as well as the acquisition of massive amounts of raw data and the extraction of critical information from both stored and real-time data. The security and privacy of data must be safeguarded.

D. Application Layer

This is the top layer of the Internet of Things. It provides a graphical user interface via which different users can access various types of applications. The applications may help health care, government, transportation, agriculture, retail, supply chain, and other industries.

IV. Application of IoT

The Internet of Things is capable of a wide variety of applications in a variety of industries. Figure.1 shows that there are numerous prominent areas where the Internet of Things has had a noticeable impact.

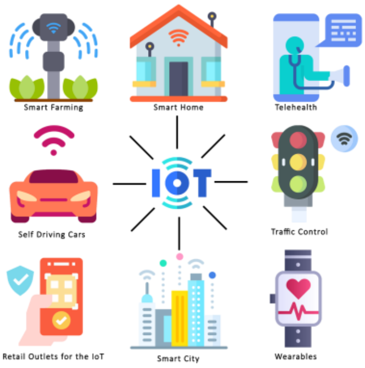

Fig.1. Applications of IoT

V. Limitations of Internet of Things

It's not as easy to protect IoT devices as it is to safeguard ordinary Internet devices. Trappe et al. [3] discussed IoT restrictions and their impact on the use of existing cryptography techniques like those used in the traditional Internet. The two principal limitations are battery capacity and processing power.

A. Increased Battery Life

Since certain IoT devices are placed in places without access to charging, they have a finite amount of energy to perform the desired functions, and hefty security instructions might deplete the gadgets' resources. Three alternative solutions exist for resolving this issue. The first choice is to use the device's minimum-security settings, which are not recommended for handling confidential material. The second option is to increase the battery's capacity. Yet, the majority of IoT devices are meant to be compact and lightweight. No more space is available for a bigger battery. The last alternative would be to gather materials from renewable resources (for example, sunlight, heat, vibration, and wind), although this would involve hardware changes and considerably raise the financial cost.

B. Lightweight Computation

According to the study [3], traditional encryption cannot be used on IoT systems because the devices' memory capacity is These authors proposed leveraging existing functionalities to implement security procedures for limited devices. For instance, physical layer authentication may be used to verify that a broadcast originated from the intended emitter in the expected location via performing signal processing at the receiver. Instead, a transmitter's unique analog characteristic can be exploited to efficiently encode analog data. These analog details are unpredictable and difficult to manage during manufacture, yet they can act as a primary identity. This method of authentication consumes very little energy due to its reliance on radio transmissions.

TABLE I. PRIVACY AND SECURITY ISSUES IN IOT

Layer of IoT	**Security/ privacy issue**	**Description**
Perception Layer (Consist of Hardware and sensors)	Lack of Proper Authentication	A huge number of RFID tags in a system might lead to concerns with security. Hackers or unauthorized individuals can view, delete, and even edit tags without permission[8] .
	Cloning Tags	Tags are cloned and placed on several objects. Hacking techniques can be used to view, read, and modify the data of objects. Tag cloning occurs when criminals can simply produce a clone of a tag and compromise it, and thus leads to tag cloning. To prevent the user from being able to tell the difference between the compromised tag and the original tag. [9]Tag authentication reduces the risk of tag cloning.
	Eavesdropping attack	When information is intercepted among pair of nodes or communication devices, this is referred as eavesdropping [10]. Data sniffing is a sort of eavesdropping. It is easy for an attacker to figure out the transfer of secret information from tag-to-reader (and vice versa) since RFID is wireless. Passive and pro-active eavesdropping attacks are the two most common in wireless surveillance, according to [11]. Pro-active eavesdropping is a technique for catching more people off guard.
	Spoofing attacks	[8] spoofing attacks are those in which an attacker tries to fool the RFID system into believing that the information they are transmitting is from a legitimate, verified and authorized source. This allows attackers to gain complete control over the machine, making it susceptible. Router routing loops are a common byproduct of spoofing attacks, according to [12]. Shortening and/or extending the source pathways is possible by repelling or enticing network nodes from the targeted nodes using this attack method. Spoofing attacks in [13] include IP spoofing and RFID spoofing, which are described in detail. It is possible for an attacker to use a genuine RFID tag's identification to collect and send malicious data, which is known as spoofing. An attack on an IoT application occurs when an attacker acts in a way that makes the application believe they are authorized users.
	Radio Frequency Jamming	Radio Frequency (RF) Jamming aims to avoid lower-level protocols in order to disrupt legal communication in [14]. RF signals can have a wide range of effects on communication by varying their patterns. In [8] an attack occurs when RFID tags are exploited by a DoS attack that distributes RF signals with noise. There are a variety of ways in which a jamming attack can be launched, and the source of the attack can either be extremely powerful or extremely weak [15].
Network Layer (Consist of protocols, communication technologies, and network)	Sybil attack	Sybil Attack: In a Sybil attack, the attacker attempts to compromise the system by changing the node's identity so that it has more than one unique identifier [8]. False information is generated by this method. Malicious objects can use several identities in the same network by displaying a fake id or an inaccurate one for any node in the network. Also, Sybil attack To trick the other IoT nodes into thinking they've been hacked into [12].
	Sinkhole attack	Compromised nodes are presented to other nodes as enticing sinkholes in a sinkhole attack [8]. As a result, all packets will be dropped when data flows across hacked nodes. Systems believe data had been sent while all other communication is halted. Because of the increased energy usage, a sinkhole attack may result in a denial of service (DoS) attack. Sinkhole attacks, in which attackers trick the system into believing that all transmitted data has been received, appear to be unidentified to the network in.
	Sleep deprivation attack	With a bad battery life, sensor nodes in the WSN suffer from sleep deprivation attacks [8]. It is because of this drawback that the sensor nodes strive to keep track of sleep schedules in order to prolong their life span. Snooze Attack works by keeping sensors awake over a period of time, which results in the battery draining, which in turn reduces battery life, prompting sensors to shut down.
	Denial of Service (DoS) attack	A denial-of-service (DoS) assault happens when an attacker attempts to overwhelm a network with a large volume of useless traffic, causing the system's resources to be depleted [8]. As a result, the system's network is no longer accessible to its users. DoS attacks occur when an attacker makes a request to a server and overloads the server, causing it to go down.
	Man in the Middle (MITM) attack	Man-in-the-middle attacks are similar to eavesdropping attacks in that the attacker places himself in the middle of the conversation. As the name suggests, a Man-in-the-Middle assault aims to compromise the communication channel, allowing an unauthorized third party to spy on and manipulate the other party [8]. A third option is for the unauthorized user to assume the victim's identity and then connect with them via the channel in order to obtain their personal data.
	Code Injection	Malicious code injection attack happens when an attacker uses a sensor node to inject malicious code into the system, causing the network to crash. In [16] code injection, an attacker can inject malicious script into an application's input field and have it run, granting the attackers access they did not have permission to have. Inserting harmful JS code into a Html file can trigger this attack, which can lead to takeover and botnet propagation.
Transport Layer (Consist of Data storage and technologies)	Unauthorized access	When an adversary erases data or prevents IoT services from accessing the IoT system, damage is done to the IoT device [8]. Both the data storage interface and the application interface are provided by the transport layer.
	Denial of Service attack	There is an enormous amount of meaningless traffic generated in a DoS attack. Attackers can temporarily disable the network's services in order to prevent the system from functioning. It is possible to launch a large number of denial-of-service attacks on the IoT system in [17]. As a result of DoS, throughput and service provider resources are exhausted. Complexity and diversity of IoT networks make it possible for DoS to infiltrate the transport layer in [18].
	Insider attack	Insiders have easy access to expand and change data for their own personal gain [8]. A malicious insider attack happens once an insider tries to interfere with data for their own or another party's gain. According to [19], one of the potential defenses against harmful insider attacks on IoT systems is the Isabelle insider framework, which may identify any policy violations.
Application Layer (Consist of Application and services)	Code Injection	Malicious code injection is the act of an attacker inserting malicious code into a system in order to steal user data, according to [8]. Attackers use XSS attacks, Trojan deployments that can block regular functioning processes, and remote code execution to take advantage of GUI flaws in software or hardware in. According to [20], anti-virus software cannot stop malicious code injection. Additionally, it has two activation options: auto or requiring the attacker to initiate an attack first.
	Denial of Service attack	DoS attacks operate on the application layer in the same manner they operate in the other layers in [17],

		with the same objective of compromising service availability. DoS attackers have the power to stop a service or application from being available in.
	Spear-Phishing attack	Spear-Phishing attacks begin when a hacker sends an email to a target and attempts to entice the recipient to open it in order to gain access to more personal information about the victim [8]. At [21], In the course of spear-phishing, an assailant gathers personal information on a single victim or a small number of individuals.
	Sniffing attack	Sniffing attacks are described in [8] as taking place when an attacker installs sniffing into the system in the form of a sniffing application, which in turn gathers network information and corrupts the system. In [22] ARP poisoning, DHCP attack, MAC flooding, and password sniffing are different types of sniffing. Mostly on data link layer, sniffers begin their work. The other top layers are also involved in the sniffing process if the data link layer is sniffer.

VI. BLOCKCHAIN

Blockchain is a novel database system meant to solve a particular set of problems. As a means of facilitating transaction processing and computing, organizations use databases as central data repositories. Businesses seldom exchange database files to prevent technological and security risks. This shared registry of transactions aims to increase transparency, safety, and efficacy [4]. The anatomy of a blockchain is as follows: This database includes transactions (among two or more entities) that have been divided into blocks (each block containing details of transactions such as the vendor, consumer, cost, contractual arrangements, and other pertinent information) and validated by the existing network via encrypted data by combining common transaction details with the distinctive signatures of multiple parties. If the block is verified and the encoding result is the same across all nodes, the transaction is valid. A "consensus" of nodes is used to fix invalid blocks.

VII. BLOCKCHAIN FUNCTIONALITY

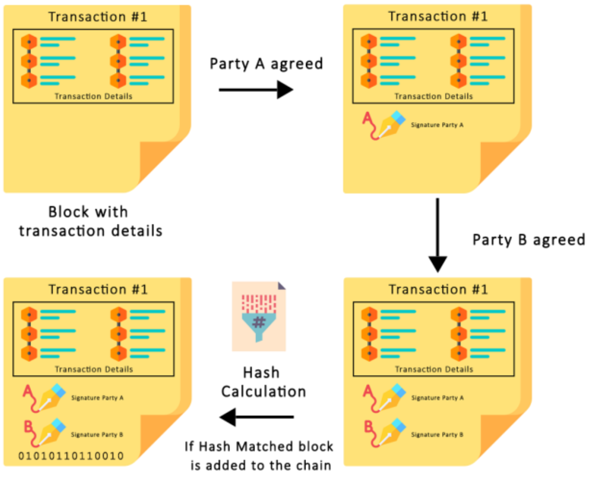

Fig.2. A diagram of construction and validation of a single blockchain block

In the present period, intermediation is the dominating method of forming holdings and completing transactions. Intermediaries do extensive due diligence on all parties involved in a chain of intermediates. This, though, is not only time-consuming and costly but also represents a credit risk in the case of an intermediary's collapse [5]. A "shift away from trusting humans and toward trusting arithmetic" is implied using blockchain technology, which eliminates the need for human contact. The figure.2 presents the overall example of a blockchain. A blockchain consists of data sets that include a chain of data packages (blocks) that each includes several transactions. The figure.3 explains how each new block is added to the blockchain, resulting in a comprehensive log of prior transactions. The network is capable of validating blocks with cryptographic methods. In addition to the transaction data, a nonce, which is a random number, is inserted into each block when a transaction is validated. This concept safeguards the whole blockchain, beginning with the very first block ("genesis block"). Moreover, because updates to a block in the chain result in a quick change in the hash value, it is simple to avoid fraud. A consensus mechanism must be in place to verify that all transactions inside a block are legitimate and that the block is valid before it can be added to the chain.

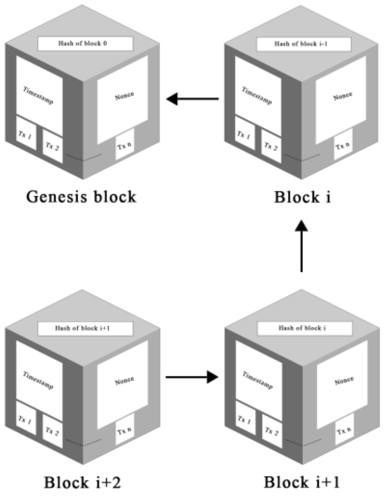

Fig.3. Example of Blockchain

Swanson [4] defines this consensus method as "the process through which a majority (or, in certain situations, all) of system validators agree on the state of a ledger." It's a set of processes and regulations that govern the organization and permits a consistent set of facts to be maintained across different participating nodes. As a result, the ledger is not automatically updated as new transactions occur. Before being entered into the ledger, the consensus process ensures that these occurrences are stored in blocks for a certain amount of time (10 minutes in Bitcoin). Thereafter, the information of the blockchain cannot be altered. Bitcoin blocks are created by so-called miners, who are compensated with Bitcoins for approving the blocks [4]. The blockchain record is dispersed among several locations, each of which is connected by a data link. This diagram illustrates a "permission" blockchain with a set number of dependable counterparties.

VIII. PRIVACY CONCERNS

For both companies and marketers, as well as other individuals, the security of an individual's private information is a top priority. If you're not paying for the goods, you're the product. This is a typical online phrase.

Consequently, firms that give free services, like social networking websites, place a great value on personal information. If information is power, then a person's ability to bargain with organizations is enhanced if that knowledge is safeguarded. Health insurers, for example, can utilize adverse health information to raise premiums or refuse coverage for specific individuals.

As a result, an individual has a reason to keep such knowledge out of the hands of the public. Health information that is made public can also have an impact on a person's personal or professional life.

Personal information can also give its owner more financial power. One may not want a bank to know about a bad credit history from several years ago, and one surely does not want criminals to utilize personal information about the individual to perpetrate identity theft or financial fraud.

Human behavior changes when they know they're being observed. Privacy, on the other hand, allows people to express themselves in a more creative, intimate, or silly way, without worry. In the same way that individuals instinctively close or lock their front doors, they want seclusion when using technology. As previously said, corporations collect personal data for a variety of purposes, including future convenience in utilizing a product or service, future ease of engagement, and researching customer preferences to build better goods. To avoid violating people's expectations of personal privacy, savvy companies make every effort to avoid violating people's expectations of personal privacy. Safeguarding confidential material, such as business strategy concepts and personal data (such as intellectual property), is critical to the success of businesses. If you're an organization that produces cutting-edge technology in your industry, you're not alone. This is true for every firm.

IX. Blockchain for the privacy and security of IoT

Blockchain is a novel database system meant to solve a particular set of problems. As a means of facilitating transaction processing and computing, organizations use databases as central data repositories. Businesses seldom exchange database files to prevent technological and security risks. This shared registry of transactions aims to increase transparency, safety, and efficacy [4]. The anatomy of a blockchain is as follows: This database includes transactions (among two or more entities) that have been divided into blocks (each block containing details of transactions such as the vendor, consumer, cost, contractual arrangements, and other pertinent information) and validated by the existing network via encrypted data by combining common

A. *Smart Home*

Connected devices have been a hot topic in academia in recent years, and it's easy to see why. For example, a smart house, a smart environment, and smart traffic control all use the IoT concept [5]. Using any of these tools does not necessitate involving a human being. The app will function in real-time using multiple sensors, actuators, and approaches. The Internet of Things (IoT) provides an app that is simple, fast, and real-time. Multiple enhancements to security have been made possible because of the block-decentralized chain's nature [6]. As a result of their potential to enable collaboration and communication, IoT devices are proliferating in practically every aspect of our lives, from growth to retail to smart homes. Smart home device traffic is used to populate a blockchain, which records a related transaction for each interaction [7].

Zhang, Jinxin Wu, and Meng [23] highlighted the effect of the COVID-19 epidemic on residential segregation. An IoT home automation system along with blockchain-based system for the safe administration of home quarantine was proposed. The use of advanced cryptographic primitives to guarantee privacy and security for a variety of events. Utilizing a PC, a laptop, a Raspberry Pi single-board computer, and the Ethereum smart contract platform, they have provided a case study of an IoT system to illustrate its use. The results indicate that it can fulfill security, efficiency, and cost-effectiveness criteria. They established a Smart Home surveillance system to monitor and report the daily in-and-out status of confined people. The method analyzes segregation using society as the fundamental unit, as opposed to individual home data. Residents' privacy and data integrity can be maintained by completing the ring signature using the public keys of other devices within the same community. Infection episodes needing special management are designated by a virtual home number, and household-specific data is encrypted with a public key before getting transmitted to pandemic prevention personnel to ensure data authenticity and security.

In their paper [24], Qashlan and his coauthors present an authentication technique that integrates attribute-based access control, smart contracts, and edge computing to provide a safe basis for IoT devices in smart home systems. The edge server enhances the scalability of the system by outsourcing expensive processing operations and collecting data into the cloud using a differential privacy mechanism. Among other issues, they study the testing and implementation of smart contracts, the differential private stochastic gradient descent technique, and system architecture and design. The authors illustrate the system's efficacy by analyzing the proposed system's privacy and security objectives in terms of confidentiality, integrity, and availability. The framework achieves the essential security and privacy requirements and is also resistant to changes, denial-of-service attacks, data mining, and link assaults. Lastly, they execute a performance review to determine the practicality and efficacy of the suggested strategy.

According to [25], the authors utilized blockchain technology in smart homes to create an encrypted and distributed ledger on which IoT data may be safely shared between several data sources. The study's security analysis found that the data protect the parameters of the ACOMKSVM model for data analysts and guarantee the confidentiality of key data from each data source. The Breast Cancer Wisconsin Data Set (BCWD) and the Heart Disease Data Set from the UCI AI repository are used to assess the suggested technique (HDD). According to simulation data, the ACOMKSVM model outperformed all other strategies in several respects.

Mohanty and co-authors presented a lightweight integrated Blockchain paradigm for the IoT in [26]. The suggested approach is demonstrated in a smart home scenario to highlight its applicability in many IoT contexts. The offered ELIB approach provides an overlay network in which highly equipped resources may be linked to form a public BC that confirms committed security and privacy. The suggested ELIB model comprises three optimizations: a lightweight consensus method, certificates (CC) cryptography, and a Distributed Throughput Management (DTM) technique. A comprehensive simulation is run under varied processing time, energy consumption, and overhead conditions. With a low energy use of 0.07mJ, the ELIB decreases total processing time by fifty percent compared to the usual technique. The trial data demonstrate that the ELIB functions optimally across a number of assessment criteria.

Qing Yang and Hao Wang have studied a wider variety of options for smart households to engage in energy transactions. Smart houses can connect with the grid to engage in vertical transactions, such as feeding surplus solar energy back into the grid and providing demand response services to ease grid strain. The usual method of transactive energy management is inefficient, compromises privacy, and has a single point of failure. To address these problems, they designed a privacy-preserving distributed algorithm [27] that enables users to best control their energy consumption in parallel using a blockchain smart contract. In addition, they designed a blockchain framework suited for IoT devices and a smart contract to enable the system's global transactive energy management. This was followed by a comprehensive evaluation of the viability and performance of the blockchain-based transactive energy management system [7] via simulations and tests. The study found that a Blockchain-based transactive energy management system can be deployed on actual IoT devices and reduces total expenses by 25%.

B. Heath Care

In the e-Health and m-Health periods, a reliable PHR system remains problematic in terms of data fusion from various EHRs, data interoperability, and ensuring that the patient has total control over data access. Alamri and colleagues [28] address these problems by establishing an electronic health wallet (EHW) system that uses new decentralized technologies such as blockchain and IPFS, as well as health data compatibility standards and technologies such as FHIR's APIs. The EHW is constructed on a platform that complies with the GDPR and offers both data security and interoperability for IoT-based PHR systems. The conceptual framework and system architecture presented here offer a comprehensive solution for a patient-centered IoT-based PHR system that maintains data privacy and meets data interoperability criteria. By encouraging patients to share their data in a regulated manner, IoT data may also be utilized for privacy-preserving health big data analytics.

The resource [29] offers an Internet of Things-enabled skin monitoring system based on blockchain-based data protection and security mechanism. The study provides a secure data transmission method for Internet of Things (IoT) devices working in a distributed architecture. At registration, a unique key is assigned to each user to secure their confidentiality. By automatically creating hash functions for each transaction variable, the blockchain concept also addresses security problems. In a decentralized setting, we employ blockchain consortiums that meet our criteria for regulated access. The presented solutions enable IoT-based skin monitoring systems to store and distribute medical data safely and securely over the network without interfering with other data transmissions.

A Blockchain and Distributed Ledger-based Improved Biomedical Security system (BDL-IBS) was designed in [30] to increase the privacy and security of healthcare data across apps. Additionally, the authors' aim is to allow patients to use the information to prove their treatment and to create strong consent systems for data disclosure across organizations and systems, as this includes managing and obtaining a large amount of healthcare data, and this technology can handle data for reliability. In conclusion, the findings imply that emerging blockchain-based digital platforms enable rapid, easy, and seamless connectivity amongst data sources, thereby enhancing privacy and data security for all stakeholders, including patients.

. In [31], M.Islam and S. Kundu propose a blockchain-based smart contract to eliminate security, trust, and privacy problems associated with IoT-enabled telematics devices in a smart home. In a smart home sharing economy, they explain how to avoid the threats posed by interior surveillance IP cameras.

To address these types of security concerns in health care, Ali and co-authors [32] developed a revolutionary security algorithm that provides both security and privacy at significantly higher efficiency and lower cost. As a result, they suggested a framework for patient healthcare in this research that delivers increased security, reliability, and authenticity when compared to existing blockchain-based access management.

The study [33] proposes a hybrid computing paradigm relying on a blockchain-based Distributed Data Storage System (DDSS) to tackle the shortcomings of blockchain-based cloud-centric IoMT healthcare systems, including excessive latency, high storage costs, and a single point of failure. To strengthen the proposed system's security features, a decentralized Selective Ring-based Access Control (SRAC) mechanism is designed, along with device authentication and patient record secrecy algorithms. The authors studied the latency and cost-effectiveness of data sharing using a Blockchain-based system. In addition, a logical system analysis was done to verify that the structure security and privacy precautions match the standards for decentralized IoMT smart healthcare systems. Compared to earlier centralized H-CPS, our Fortified-Chain-based H-CPS utilizes less memory and has a millisecond reaction time, while enabling decentralized automation access control, security, and privacy.

C. Fog computing

In [34], it was proposed to deploy an Ant Colony Optimization (ACO) method in combination with a Fog-enabled Blockchain-assisted scheduling paradigm, dubbed PF-BTS. PF-protocol BTSs and algorithms use BC miners to efficiently distribute work to cloud-based virtual machines (VRs) through ACO and to compensate miner nodes for their contribution to setting the optimal schedule. In addition, PF-approach BTSs enable the fog to assess, manage, and conduct tasks to enhance latency metrics. During this processing and management, the fog is enforced to safeguard the privacy of system components and to prevent the disclosure of data, geolocation, identity, and use information. In a simulated setting, they analyze and compare the performance of PF-BTS with that of a recently introduced Blockchain-based task scheduling system. Our review and testing demonstrate that PF-BTS has a high level of privacy awareness, as well as a considerable improvement in execution time and network load.

Zhang and his colleagues [35] present a privacy-aware authentication method for multi-server CE-IoT systems by merging PUFs with blockchain technology. The genuine relationships of CRPs are double-encoded into mapping correlations employing a one-time physical identifier and a keyed-hash method (MCs) (MCs). The blockchain is utilized to securely store MCs, sync them, and express the physical identity using multi-receiver encryption. The security of the protocol is defined using a randomized oracle model, and the protocol's resistance to a range of attacks is demonstrated using security characteristics. In addition, a prototype was created to illustrate the efficacy of the protocol, and comparison results indicate that our protocol is acceptable with CE-IoT systems. Lastly, the modeling of the smart contract proves the scalability of our system.

Based on blockchain technology, [35] provides a distributed access control strategy for IoT data security. The presented technique is built on fog computing and the concept of an alliance chain. This strategy encrypts Data or information on an edge node using mixed linear and nonlinear spatiotemporal chaotic systems (MLNCML) and the least significant bit (LSB) and then submits the encrypted data to the cloud. The recommended technique can address the problem of a system failure in access control by enabling dynamic and granular access control for IoT data. The testing results indicated that this technique is capable of maintaining the confidentiality of IoT data.

The study [36] offers a blockchain-based hybrid algorithm to solve the inefficiencies of existing privacy methods. Prior to outsourcing data to computer servers, it is encrypted using a revolutionary hybrid approach, and a unique digital signature is formed and kept at the client on a set of decentralized blocks. To validate the proposed architecture, a virtual cloud imitating genuine cloud service infrastructure was developed. Despite the additional processing power taken to accomplish the proposed framework due to the blockchain integration, the findings reveal that data integrity and reliability are preserved while user privacy is increased. Examining and comparing the results to established criteria for privacy verification, including modifications in stored data, low overhead on cloud efficiency, and the data record structure of the blockchain

D. Smart contracts

According to blockchain technologies and cyber-physical systems, conventional industrial processes, technological methods, and business models are being upgraded. It utilizes frame resilience and intelligent contracts to reduce the complexity of service costs. Blockchain applications integrate fundamental features of self and self-integrity to eliminate the need for trusted third parties. It converts scientific and industrial advances into Industry 4.0, which uses Artificial Intelligence (AI) to evaluate and extract useful data from real-time systems. In addition, digital analytics is utilized to combine data with blockchain and cloud storage in order to improve system efficiency. Concerns about security and privacy make it challenging to investigate AI concepts and technologies. Consequently, [37] presents a privacy-protecting smart contract architecture (PPSC-BCAI) that simplifies human contact, system actions, service warnings, cyber-attacks, and fraudulent claims. Extreme gradient boosting (XGBoost) is used to examine data sharing and transactions. It evaluates the transaction service to reduce network stress, revealing whether the transmission rate fluctuates due to unstable network connectivity.

Loukil [38] suggested a revolutionary IoT device management paradigm that stresses privacy and is based on blockchain technology. In the proposed system, IoT devices are managed by many smart contracts that validate the connection permissions based on the data owners' privacy authorization settings and the array of IoT device misbehavior records that have been saved. In actuality, smart contracts can identify quickly devices that are vulnerable, hacked, or pose a threat to the IoT network. Consequently, the privacy of the data owner is protected by imposing control on one's own devices. They validate the offered solution by installing it on a personal Ethereum blockchain and evaluating its performance.

In [39], the authors present PETchain, an innovative privacy-enhancing blockchain and smart contracts-based platform. PETchain stores information in a secure, decentralized manner and processes it in a user-selected, trusted execution environment. Users participate in the smart contract, which allows them to select if and how service providers use their data. PETchain's usability and performance are demonstrated by its implementation on a consortium Ethereum blockchain.

[40] outlines a system that employs Dynamic Access Control and Fair Access. The entire fair access procedure is documented in a smart contract, and token allocation may be done via Digital Signature. This improves the system's performance. The goal of incorporating Blockchain into accounting rules is to guarantee that auditors are performing to their full ability in terms of checking accounts and financial records in line with International Accounting Standards. This approach aims to reduce the number of minor workplace scams, which might lead to the business's demise if the privacy of smart contracts is improved.

E. Smart cities

Makhdoom and his colleagues created "PrivySharing," a blockchain-based framework for the secure and private sharing of IoT data in a smart city environment. The proposed system [41] varies from earlier methods in several respects. The data privacy is preserved by segmenting the chain of blocks into numerous channels, each of which handles a specific sort of data, such as health, smart cars, smart energy, or financial data, and has a restricted number of permitted organizations. Moreover, entry to individuals' information within a channel is governed by access control rules included in smart contracts. In addition, information inside channels is separated and protected through the use of private data collection and encryption. Likewise, the REST API that enables clients to connect to the blockchain employs both an API Key and OAuth 2.0 for protection. The proposed solution conforms with a number of the main requirements outlined in the EU's General Data Protection Regulation. We also offer a compensation plan for users who disclose personal information with stake-holder parties in the form of "PrivacyCoin" virtual currency. The results indicate that a multi-channel blockchain system is more scalable than a single-channel blockchain system.

The Trustworthy Privacy-Preserving Secured Framework (TP2SF) is described in [42]. This design includes trustworthiness, two-level privacy protection, and IDS. The address-based blockchain reputational system is implemented within the module for trustworthiness. Data is changed into a new reduced shape in the two-level privacy module utilizing blockchain-based enhanced Proof of Work (ePoW) and Principal Component Analysis (PCA) to resist inference and poisoning attacks. The intrusion detection module uses an extended gradient tree boosting algorithm (XGBoost). Due to the Fog-Cloud architecture's inherent advantages and disadvantages, a blockchain-IPFS integrated Fog-Cloud architecture, CloudBlock, and FogBlock, was developed to implement the proposed TP2SF framework in smart cities. To evaluate the TP2SF framework, the ToN-IoT and BoT-IoT IoT-based datasets are utilized. The outcomes demonstrate that the TP2SF framework outperforms current state-of-the-art approaches in non-blockchain and blockchain environments.

Sarac and his coauthors offer a method for giving a basic API to the security gateway design of an Internet of Things (IoT) device with Blockchain for decentralization and authentication. The current IoT infrastructure lacks anonymity and flexibility, which are provided by [43]. Data credibility of assured by appropriate cryptography. Microgrid trade may be launched, data can be transmitted securely across 5G or 6G network architectures, and the system is compatible with any IoT devices. Additionally, it can run any cryptographic method on data. As part of this project, a security mechanism that supports all cryptographic methods for all IoT devices on the network has been established. In addition, the interface is secured by Blockchain technology, which removes a single point of control, archives previous transactions performed by IoT devices, and assures device trust.

X. Conclusion

To protect the IoT system, blockchain technology could be utilized. This connection can be used to define policies and monitor activity with smart contracts. Combining blockchain and IoT will yield substantial outcomes. The Internet of Things is strengthened by blockchain as it provides trustworthy sharing services and traceable data. When utilizing Blockchain, the primary information may be identified, hence enhancing security. Therefore, Blockchain serves as a strategy for securing and enhancing the Internet of Things. Therefore, single point failure is a significant threat to the Internet of Things. Blockchain may be used to substitute the central server with a decentralized network and distributed file system [44] to address this issue. Blockchain contributes to the creation of a stable system by enhancing the anonymity of Internet of Things (IoT) technologies. It facilitates device coordination as well. The distributed ledger of Blockchain enables accurate data verification and interpretation. The marriage of blockchain and IoT enhances the IoT system's security and dependability.

There are a few challenges that occur when combining Blockchain with IoT. Limitations such as a lack of competent personnel, correct legal difficulties, a lack of storage capacity, variations in computer skills, restricted technological improvements, computing capabilities, processing time, and scalability issues all contribute to the obstacles [45]. Although this integration is crucial, the essence of both technologies is extremely different. Blockchain was created with powerful computers in mind, but the reality of IoT is quite different. Storage capacities, the scale of blockchain has still been experiencing certain concerns, and thus appears to be unsuitable for IoT applications are some of the obstacles that occur because of this integration. IoT devices create enormous amounts of data, but current blockchain technology can only execute a few transactions per second, posing a significant problem for the IoT. Other challenges with Blockchain are legal issues, such as rules governing information processing and privacy concerns, which must be addressed in the IoT. There are several benefits to utilizing blockchain with IoT, but only if we utilize it responsibly and with adequate caution will it become a benefit for protecting IoT. Blockchain has the potential to change the Internet of Things by assisting in the improvement of IoT applications. The combination of blockchain with IoT overcomes a slew of problems that plague the IoT system. The contact between citizens, businesses, and the government is accelerated because of this integration [46].

References

[1] J. Sengupta, S. Ruj, and S. Das Bit, “A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT,” *J. Netw. Comput. Appl.*, vol. 149, p. 102481, 2020, doi: 10.1016/j.jnca.2019.102481.

[2] M. Sadrishojaei, N. J. Navimipour, M. Reshadi, and M. Hosseinzadeh, “A New Preventive Routing Method Based on Clustering and Location Prediction in the Mobile Internet of Things,” *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10652–10664, 2021, doi: 10.1109/JIOT.2021.3049631.

[3] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012, doi: 10.1016/j.adhoc.2012.02.016.

[4] Z. Ghanbari, N. Jafari Navimipour, M. Hosseinzadeh, and A. Darwesh, “Resource allocation mechanisms and approaches on the Internet of Things,” *Cluster Comput.*, vol. 22, no. 4, pp. 1253–1282, 2019, doi: 10.1007/s10586-019-02910-8.

[5] C. Ge, Z. Liu, and L. Fang, “A blockchain based decentralized data security mechanism for the Internet of Things,” *J. Parallel Distrib. Comput.*, vol. 141, pp. 1–9, 2020, doi: 10.1016/j.jpdc.2020.03.005.

[6] C. Perera, C. H. Liu, and S. Jayawardena, “The Emerging Internet of Things Marketplace from an Industrial Perspective: A Survey,” *IEEE Trans. Emerg. Top. Comput.*, vol. 3, no. 4, pp. 585–598, 2015, doi: 10.1109/TETC.2015.2390034.

[7] D. Bandyopadhyay and J. Sen, “Internet of things: Applications and challenges in technology and standardization,” *Wirel. Pers. Commun.*, vol. 58, no. 1, pp. 49–69, 2011, doi: 10.1007/s11277-011-0288-5.

[8] M. U. Farooq and M. Waseem, “A Critical Analysis on the Security Concerns of Internet of Things (IoT),” vol. 111, no. 7, pp. 1–6, 2020.

[9] B. Khoo, “RFID as an Enabler of the Internet of Things : Issues of Security and Privacy,” 2011, doi: 10.1109/iThings/CPSCom.2011.83.

[10] F. A. Alaba, M. Othman, A. T. Hashem, and F. Alotaibi, “Author ’ s Accepted Manuscript Internet of things Security : A Survey Reference :,” 2017, doi: 10.1016/j.jnca.2017.04.002.

[11] H. Lu, “Proactive eavesdropping in UAV-aided mobile relay systems,” 2020.

[12] H. I. Ahmed, A. A. Nasr, S. Abdel-mageid, and H. K. Aslan, “A survey of IoT security threats and defenses A survey of IoT security threats and defenses,” no. October, 2019, doi: 10.19101/IJACR.2019.940116.

[13] A. Kamble and S. Bhutad, “SURVEY ON INTERNET OF THINGS (IOT),” *2018 2nd Int. Conf. Inven. Syst. Control*, no. Icisc, pp. 307–312, 2018.

[14] C. Pereira and A. Aguiar, “A Realistic RF Jamming Model for Vehicular Networks : Design and Validation,” pp. 1868–1872, 2013.

[15] N. Of, “A s s i w s n,” pp. 2–23, 2006.

[16] V. Rq *et al.*, “$ vxuyh\ rq &rgh ,qmhfwlrq $wwdfnv lq 0reloh &orxg &rpsxwlqj (qylurqphqw,” pp. 135–140, 2018.

[17] R. Roman, J. Zhou, and J. Lopez, “On the Features and Challenges

of Security & Privacy in Distributed Internet of Things," vol. 57, 2013.

[18] "[PDF] Evaluating Critical Security Issues of the IoT World: Present and Future Challenges | Semantic Scholar." https://www.semanticscholar.org/paper/Evaluating-Critical-Security-Issues-of-the-IoT-and-Frustaci-Pace/6d464bd9075daaa88e8aba1fca56e7ce74dd43c3 (accessed Jul. 24, 2022).

[19] A. Y. Khan, R. Latif, S. Latif, S. Tahir, G. Batool, and T. Saba, "Malicious Insider Attack Detection in IoTs Using Data Analytics," *IEEE Access*, vol. 8, pp. 11743–11753, 2020, doi: 10.1109/ACCESS.2019.2959047.

[20] M. Burhan, R. A. Rehman, B. Khan, and B. S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," *Sensors (Switzerland)*, vol. 18, no. 9, pp. 1–37, 2018, doi: 10.3390/s18092796.

[21] L. Allodi, T. Chotza, E. Panina, and N. Zannone, "The Need for New Antiphishing Measures against Spear-Phishing Attacks," *IEEE Secur. Priv.*, vol. 18, no. 2, pp. 23–34, 2020, doi: 10.1109/MSEC.2019.2940952.

[22] P. Anu and S. Vimala, "A survey on sniffing attacks on computer networks," *Proc. 2017 Int. Conf. Intell. Comput. Control. I2C2 2017*, vol. 2018-Janua, pp. 1–5, 2018, doi: 10.1109/I2C2.2017.8321914.

[23] J. Zhang and M. Wu, "Blockchain use in iot for privacy-preserving anti-pandemic home quarantine," *Electron.*, vol. 9, no. 10, pp. 1–16, 2020, doi: 10.3390/electronics9101746.

[24] 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.

[25] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the internet of things," *IEEE Secur. Priv.*, vol. 13, no. 1, pp. 14–21, 2015, doi: 10.1109/MSP.2015.7.

[26] S. N. Mohanty *et al.*, "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy," *Futur. Gener. Comput. Syst.*, vol. 102, pp. 1027–1037, 2020, doi: 10.1016/j.future.2019.09.050.

[27] Q. Yang and H. Wang, "Privacy-Preserving Transactive Energy Management for IoT-Aided Smart Homes via Blockchain," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11463–11475, 2021, doi: 10.1109/JIOT.2021.3051323.

[28] B. Alamri, I. T. Javed, and T. Margaria, "A GDPR-Compliant Framework for IoT-Based Personal Health Records Using Blockchain," *2021 11th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2021*, 2021, doi: 10.1109/NTMS49979.2021.9432661.

[29] S. Juyal, S. Sharma, A. Harbola, and A. S. Shukla, "Privacy and Security of IoT based Skin Monitoring System using Blockchain Approach," *Proc. CONECCT 2020 - 6th IEEE Int. Conf. Electron. Comput. Commun. Technol.*, 2020, doi: 10.1109/CONECCT50063.2020.9198409.

[30] H. Liu, R. G. Crespo, and O. S. Martínez, "Enhancing privacy and data security across healthcare applications using Blockchain and distributed ledger concepts," *Healthc.*, vol. 8, no. 3, 2020, doi: 10.3390/healthcare8030243.

[31] M. N. Islam and S. Kundu, "IoT security, privacy and trust in home-sharing economy via blockchain," *Adv. Inf. Secur.*, vol. 79, no. November, pp. 33–50, 2020, doi: 10.1007/978-3-030-38181-3_3.

[32] A. Ali *et al.*, "Security, privacy, and reliability in digital healthcare systems using blockchain," *Electron.*, vol. 10, no. 16, pp. 1–27, 2021, doi: 10.3390/electronics10162034.

[33] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11717–11731, 2021, doi: 10.1109/JIOT.2021.3058946.

[34] H. Baniata, A. Anaqreh, and A. Kertesz, "PF-BTS: A Privacy-Aware Fog-enhanced Blockchain-assisted task scheduling," *Inf. Process. Manag.*, vol. 58, no. 1, p. 102393, 2021, doi: 10.1016/j.ipm.2020.102393.

[35] Y. Zhang, B. Li, B. Liu, Y. Hu, and H. Zheng, "A Privacy-Aware PUFs-Based Multiserver Authentication Protocol in Cloud-Edge IoT Systems Using Blockchain," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 13958–13974, 2021, doi: 10.1109/JIOT.2021.3068410.

[36] M. A. Darwish, E. Yafi, M. A. Al Ghamdi, and A. Almasri, "Decentralizing Privacy Implementation at Cloud Storage Using Blockchain-Based Hybrid Algorithm," *Arab. J. Sci. Eng.*, vol. 45, no. 4, pp. 3369–3378, 2020, doi: 10.1007/s13369-020-04394-w.

[37] H. Li, D. Han, and M. Tang, "A Privacy-Preserving Charging Scheme for Electric Vehicles Using Blockchain and Fog Computing," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3189–3200, 2020, doi: 10.1109/jsyst.2020.3009447.

[38] F. Loukil, C. Ghedira-Guegan, K. Boukadi, A. N. Benharkat, and E. Benkhelifa, "Data Privacy Based on IoT Device Behavior Control Using Blockchain," *ACM Trans. Internet Technol.*, vol. 21, no. 1, pp. 1–20, 2021, doi: 10.1145/3434776.

[39] I. T. Javed, F. Alharbi, T. Margaria, N. Crespi, and K. N. Qureshi, "PETchain: A Blockchain-Based Privacy Enhancing Technology," *IEEE Access*, vol. 9, pp. 41129–41143, 2021, doi: 10.1109/ACCESS.2021.3064896.

[40] R. Gupta, V. K. Shukla, S. S. Rao, S. Anwar, P. Sharma, and R. Bathla, "Enhancing privacy through 'smart contract' using blockchain-based dynamic access control," *Proc. Int. Conf. Comput. Autom. Knowl. Manag. ICCAKM 2020*, pp. 338–343, 2020, doi: 10.1109/ICCAKM46823.2020.9051521.

[41] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities," *Comput. Secur.*, vol. 88, p. 101653, 2020, doi: 10.1016/j.cose.2019.101653.

[42] P. Kumar, G. P. Gupta, and R. Tripathi, "TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning," *J. Syst. Archit.*, vol. 115, p. 101954, 2021, doi: 10.1016/j.sysarc.2020.101954.

[43] M. Šarac, N. Pavlović, N. Bacanin, F. Al-Turjman, and S. Adamović, "Increasing privacy and security by integrating a Blockchain Secure Interface into an IoT Device Security Gateway Architecture," *Energy Reports*, vol. 7, no. xxxx, pp. 8075–8082, 2021, doi: 10.1016/j.egyr.2021.07.078.

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

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

[46] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," *J. Netw. Comput. Appl.*, vol. 125, no. March 2018, pp. 251–279, 2019, doi: 10.1016/j.jnca.2018.10.019.