# IoT access control with blockchain technology: current practices and future directions



[1]Jorair Ahmad, Department of Information Technology and Security, College of Computer Science and information technology, Jazan University, Jazan, Saudi Arabia, Email: jorair@jazanu.edu.sa
[2]Syed Ghyasuddin Hashmi, Department of Information Technology and Security, College of Computer Science and Information Technology, Jazan University, Jazan, 45142, Saudi Arabia, Email: shashmi@jazanu.edu.sa
[3]Khalid Ali Qidwai, Department of Computer Science, College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia, Email: khalidqidwai@gmail.com
[4]Ziauddin Syed, Department of Computer Science, College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia, Email: ziauddin@jazanu.edu.sa
[5]M. Sahithullah, Associate Professor, EEE Department, Er. Perumal Manimekalai College of Engineering, Hosur – 635117, Email: sahithullahmahaboob@gmail.com
[6]Ikhsan, Akademi Manajemen Informatika & Komputer Jaya Nusa Padang, Indonesia, Email: riksjp21@gmail.com
[7]Rupendeep Kaur, Assistant professor, Department of electronics technology, Guru Nanak dev university, Amritsar, Email- rupendeep.ece@gndu.ac.in
[8]Samuel-Soma M. Ajibade, Dept of Computer Engineering, Faculty of Engineering, Istanbul Ticaret Universitesi, Istanbul, Turkey, asamuel@ticaret.edu.tr

**ABSTRACT**

Internet of Things (IoT) applications and services have become increasingly prevalent due to the fast evolution of wireless sensor networks, smart devices, and conventional information and communication technology. The data processed by IoT systems is enormous. This information may be extremely delicate because it relates to private matters such as health, finances, and whereabouts. Therefore, strong access control is essential for IoT's granular security management. Several solutions have been proposed to handle security for the Internet of Things. Although blockchain-based approaches are being developed for IoT access control, they are very briefly referenced. In this article, we look at the growing interest in and need for IoT access control systems that are built on the blockchain. In this article, we examine the pros and cons of using blockchain technology to get access to the Internet of Things, including distributed systems, safe data management, and trustless information exchange. Finally, we highlight several promising areas for further study on the merging of blockchain technology with Internet of Things networks.

**KEYWORDS**: Internet of Things, Blockchain, Security, Trust, Access control, Identity

**DOI Number: 10.14704/NQ.2022.20.15.NQ88464** **NeuroQuantology2022;20(15): 4599-4615**

## 1. INTRODUCTION

The Internet of Things (IoT) encompasses a huge number of networked devices, tools, people, and decentralized parts of smart systems. 50 billion IoT-connected products will be in use by 2022 [1], a result of the exponential expansion of the IoT network. This will lead to an increase in the typical family's total number of connected gadgets and Internet users. In addition, annual worldwide traffic is anticipated to hit 3.3ZB (Zettabyte) by the middle

of 2021. While more IoT apps mean lower application costs and better treatment, they also increase the system's vulnerability to attack [2]. One of the most important aspects of Internet of Things security is access control. The purpose of access control is to limit access to protected resources to those who are explicitly allowed to do so by a predetermined set of rules. If specific criteria are satisfied, it places restrictions on which entities can make use of which resources [3]. In Figure 1 we see a simplified version of the typical access control flow. Because of their mobility, low computing power, and short battery life, IoT devices are especially susceptible to network attacks [4]. This heightened risk is due to the fact that well-established traditional security procedures cannot be immediately applied to low-resource IoT devices.

### 1.1. An explanation of the problem and its origins

More so, due to the vastness and variety of IoT networks, it is challenging to define precise and comprehensive access policy settings in advance for users and devices. Role-based access control (RBAC), attribute-based encryption access control (ABAC), and functionality-based access control (CapBAC) are widely used in modern IoT access control systems [5]. Role-based access control (RBAC) regulates the assignment of users to jobs and grants some discretion over resource permissions. To implement RBAC, a distinct user-to-permission connection must be specified for each resource. The high degree of concentration in RBAC makes it impractical for use in big, complicated systems like IoT. Attribute management and enforcing granular access constraints in IoT systems are hence made more challenging.

Instead, then focusing on the unique physical IDs of things, ABAC uses their qualities to facilitate better policy administration (e.g., place, date, time, etc.). This is promising since it indicates that the policies were drafted keeping the situation in mind. This allows for granular control over policy administration in an IoT program, but ABAC doesn't specify how several policies are needed. To rephrase, ABAC does not provide mechanisms for aggregating policies that grant access to the same resource and have distinct information requirements, or policies that have the same legacy includes but grant access to separate resources. A plan management system is crucial for ABAC, particularly as the number if policies develop dramatically, to ensure effective resource usage permission enforcement [6].



The modular transfers of access control techniques is made more difficult in an IoT system due to the need to define a set of qualities that are particularly authorized for each user, item, and service. Distributing capabilities tokens, which are also referred as permission tokens and include access rights or privileges, is how CapBAC enables flexible access control. In order to ensure that only authorized users have access to a given resource, edge IoT devices can check the validity of these tokens. In this scenario, those kinds are not needed to maintain intricate policy stacks. Although most CapBAC systems store and administer policies in a single location [7], others do not. This further complicates scalability issues with attribute management and user access transfer.

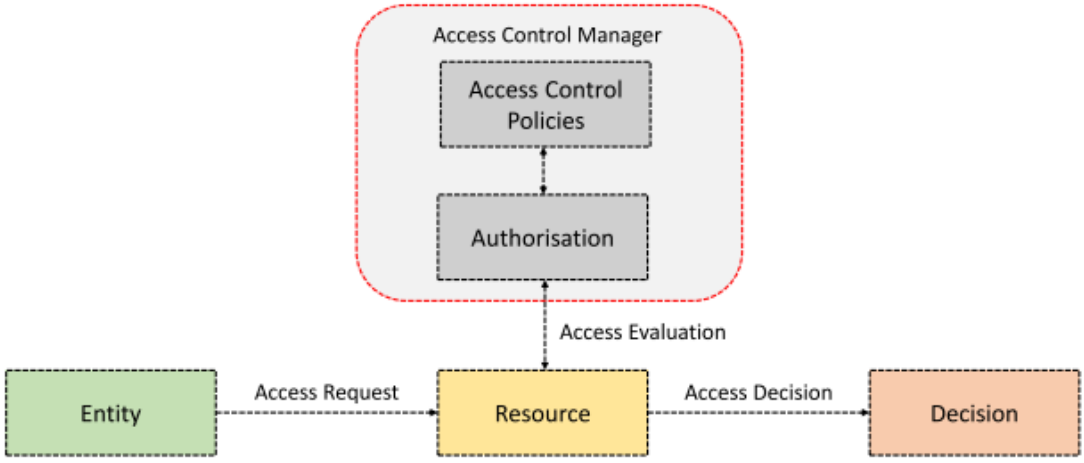


**Figure1: The main functional elements and how they interact during the access control process [1]**

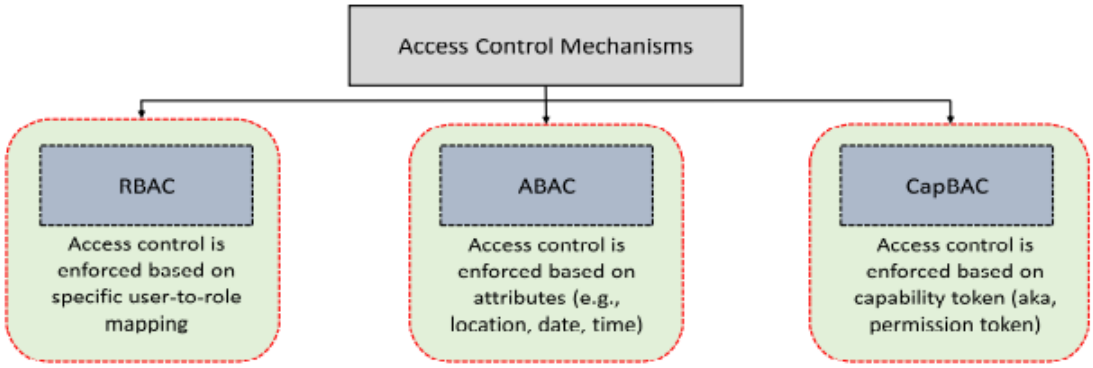


**Figure 2: Methods of IoT access control that are frequently used [1]**

The foregoing examination uncovered five essential features of IoT access control mechanisms: (1) resource management; (2) transfer of access rights; (3) enforcement of permissions; (4) attribute management; and (5) scalability. In large-scale Web of Things systems, these five features are crucial for designing access control, including resource management, monitoring access control policies with suitable security measures, and giving access permissions to various organizations. In Section 3.2, we go into further depth about these classifications. In order to efficiently supply network access to electronic devices and block unwanted users, the bulk of existing data access options only sufficiently cover some of these aspects with limited data.

We stress the need of thinking about access control in IoT early on in the design process so that they may be used to enforce policies in a way that is scalable, efficient, lightweight, reliable, and robust. Decentralized management techniques are required for IoT networks due to their scale and diversity [8]. The limitations of existing access control techniques (such RBAC, ABAC, and CapBAC) for large-scale IoT systems operating across different countries have been increasingly apparent in recent years [9], and blockchain technology has emerged as a viable solution. Access control for Internet of Things devices via a blockchain is illustrated conceptually in Figure 3. Blockchain paves the way for new possibilities by offering a distributed ledger and a computational platform for any software. The blockchain offers a



eISSN 1303-5150

safe and secure method of recording transactions in a decentralized manner throughout the network because to its qualities, such as the absence of centralized control and a trusted third party, the consensus protocol, immutability, inevitability, and tamper-proofness. Inadequate measures for controlling user access are required by the system [10].



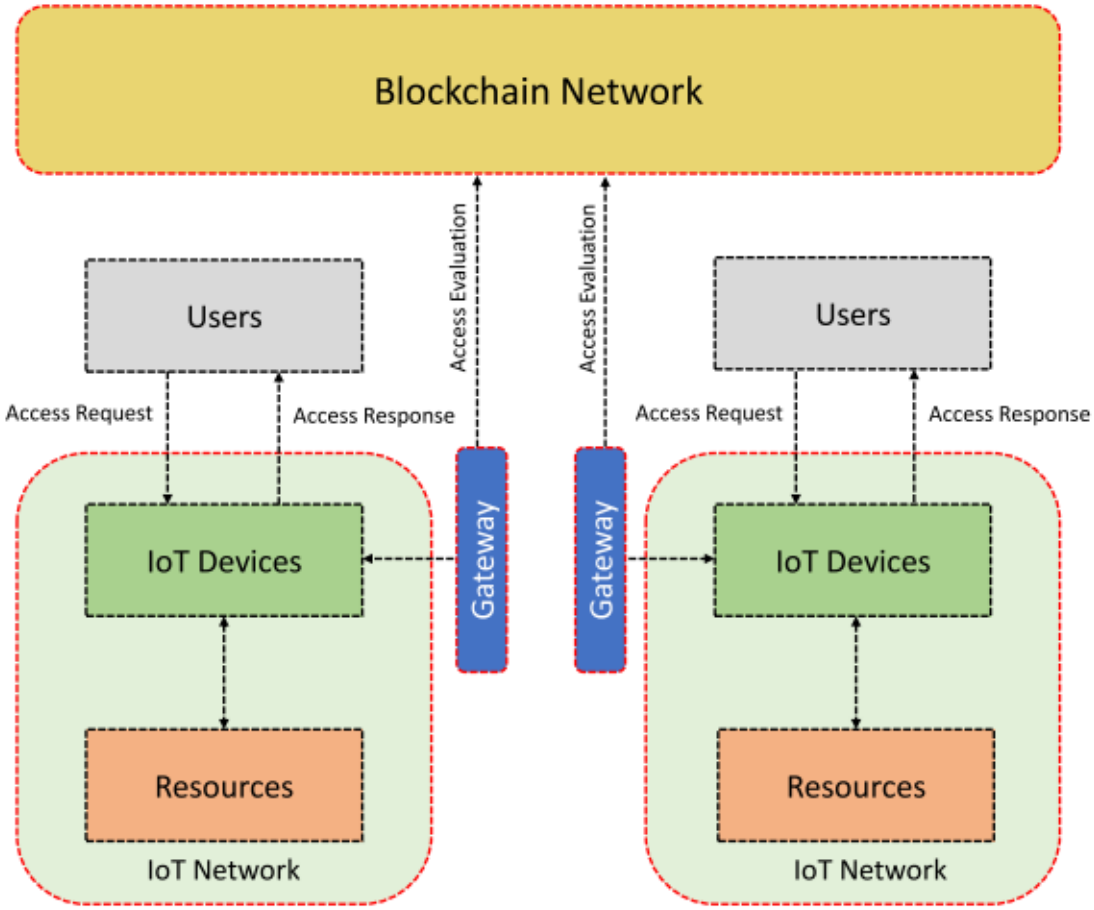


**Figure 3: Access control in IoT based on blockchain technology [1]**

**Table 1 List of abbreviations used in the paper and their full name.**

| Abbreviations | Full name |
|---|---|
| IoT | Internet of things |
| RBAC | Role-based access control. |
| ABAC | Attribute-based access control |
| CapBAC | Capability-based access control |
| AC | Access control |
| BC | Blockchain |
| DDoS | Distributed denial-of-service |
| PoW | Proof-of-work |
| CoAP | Constrained application protocol |
| REST | Representational state transfer |
| LSB | Light-weight scalable blockchain |
| IETF | Internet engineering task force |

| | |
|---|---|
| DTM | Distributed throughput management |
| CP-ABE | Cipher-policy attribute-based encryption |
| CH | Cluster heads |
| XDK | Cross-domain development kit |
| HDAC | Hyundai digital asset company |
| URL | Uniform resource locators |
| PBFT | Practical byzantine fault tolerance |
| AI | Artificial intelligence |
| ML | Machine learning |

**1.2. Organization and planning**

Here is how the rest of a essay is structured. The significance of network accessibility for IoT systems is discussed in Section 2 of this article. IoT access control needs are discussed in this section. The methods of securing the Internet of Things using blockchain technology are outlined in Section 3. First, we'll have a quick overview of blockchain technology. We next conduct an evaluation of these options by classifying the different ways in which the present solutions for securing ledger-based Internet of Things user access deal with the problem of unauthorized access. Within this section, we review the information presented in Chapter 4. Towards the end of the paper, we will discuss the next paths of study (Section 5). Subsequently, the article finishes with Section 6. The entire names of all acronyms shown in this study are given in Table 1.

**2. Importance of access control in IoT**

There's been a huge increase in the demand for the consumption of smart devices over the past decade [11], largely as a result of the proliferation of IoT technologies. In addition, the sensing, thinking, and communicating capabilities of smart IoT devices increase the likelihood that they will be used in a wide range of contexts. As a result, anything and everything can become a part of the network (e.g., Through the Internet). It highlights the widespread use of instrumentation and the integration of smart devices [12]. As a result, it's important to understand how objects in the IoT ecosystem might interact with one another, as these interactions frequently take place under murky circumstances [13]. A thing can be thought of as a singular entity or as a grouping of people, devices, software, and services. Things may become highly mobile or move between different network domains. Proper policies for access control and mechanisms are necessary to enable secure interaction and make sure that data can be decided to share only with authorized things. It is possible that access control policies will occasionally be implemented in real time. The data processed by IoT systems is enormous. The health, location, and other personal details that may be included in this data make it especially delicate. In order to regulate who has access to what information and how, devices connected to the Internet of Things (IoT) must implement access control measures. In order to facilitate data sharing, it is common practice for one organization to grant access to another. Delegation is the act of giving someone else authority over some resource and the rules for regulating that authority. The one doing the handing over is called the instructor, while the one getting the instruction is called the delegate.

Delegating authorized users in an IoT context is challenging due to the aforementioned features of the system, such as movement, resource restrictions, scalability, and so on. The assignment of access privileges is described in depth in Section 3.2.2. Delegation of reasonable access requires correct implementation in a wide dispersed network like the IoT to prevent any security risks caused by data that is manipulated or stolen. Factors like (1) item authenticity, (2) trust leaders between devices and



eISSN 1303-5150

users, (3) wireless sensor domains, (4) visibility in written consent for responsible interoperability to IoT funds, and (5) lively network topology, where conversations between both things may only occur once or for a very short period of time, are all potential vulnerabilities in the IoT. These power sources are vulnerable to attack even when there is no internet connection, keeping devices from updating to the most secure versions of software. Traditional security procedures have difficulty protecting an IoT system from possible risks and assaults because of characteristics unique to the IoT, such as its openness, data freshness, and self-healing [14,15].

Security and privacy attacks on traditional computer systems are very different from IoT assaults. Attacks are growing more sophisticated in terms of their procedures and how they infect the scheme because of the IoT's distinctive traits, such as dynamic interactions, heterogeneity in systems and services, and limited memory, storage, and battery capacity. This goes beyond merely putting malicious software into a network layer or stealthily rerouting traffic to an unsecured location.

Instances when an Internet of Things (IoT)-enabled medical product can be compromised and remotely operated are increasingly readily apparent. A patient's pacemaker may be used to provide a fatal shock, or an attacker could seize control of a medicine infusion pump (for antibiotics or insulin, for example) and alter the drug dose while having allowed access [16]. In 2016, a widespread DDoS (Distributed Denial-of-Service) assault known as the "Mirai Botnet" [17] infiltrated numerous IoT devices, primarily outdated routers and IP cameras, and inundated them with internet traffic (Anon, 2020a). The "Cayla" doll was banned [18] in Germany in 2017 on major safety and privacy issues. Cayla is an intelligent Internet of Things doll that helps kids learn. By engaging in conversation and taking an interest in their ideas, you can provide them a unified play experience. However, privacy might be compromised owing to the dolls' inherent weakness and the Bluetooth connection's lack of encryption. In 2016, a distributed denial of service (DDoS) [19] attack rendered all of Finland's central heating and hot water networks inoperable. These events illustrate the variety of outcomes that can result from the penetration of a typical IoT device and its exploitation to break into and attack bigger networks.



Therefore, it is crucial to take necessary precautions to secure IoT systems and to enforce suitable access control regulations. In addition, access control needs to be positioned such that it can readily communicate with devices at the periphery of the Internet of Things. To govern access to resources efficiently while adhering to as few rules as feasible, a considered to be a vital is necessary [20]. Avoiding and controlling the flow of illegal information and developing proper safety protocols for IoT identity management are essential for laying a solid security base for an IoT system. Existing authorization workarounds for the Internet of Things, as was previously mentioned, must not pony up adequate attention to key access control needs including decentralization of control, disclosure in the application of access management, and trying to address trust between agencies at a finer level. Regrettably, the majority of the existing proposals' strategies for controlling access have a common weak spot. Even more frequently in written plans of this sort is the adoption of a single, specified approach for reviewing policies.

## 3. Blockchain-based solutions for IoT access control

Here, after a quick review of blockchain technology, we demonstrate the numerous cryptocurrency network access methods for IoT devices that have been proposed in recent publications.

### 3.1. Blockchain technology

Bitcoin, the first cryptocurrency, uses blockchain as its underlying technology [21]. With blockchain, even if some of the nodes in a network

can't be trusted, the rest of the network can verify any and all transactions or conversations between nodes. Because all nodes in a blockchain may take part in a transaction and a block, centralized controllers are unnecessary. Blockchain's ability to manage decentralized data comes from the fact that all nodes maintain a chronological log of all transactions in a "block" format. Each block in the blockchain keeps a copy of the hash from the prior block in the ledger, making it possible to identify any tampering with the original data. The term "genesis block" is used to describe the very first entry in the ledger. Time stamps are used to create a logical chain between the continuing blocks (i.e., blocks that have been recently added) and the rest of the network. Network nodes that adhere to a consensus process are referred to be miners or validators. They compile recently completed trades into a new "block" that is added to the coin. All nodes must go through two stages before they can reach consensus on the ledger's legitimate state, and this is handled by the consensus process. (1) consensus in the ledger: because to the decentralized structure of the blockchain, it is possible for different nodes to produce the same block at the same time, leading to a split in the network. (2) Verification selection: this process, which involves deciding which validator will verify the next block, is referred to in the literature as the consensus algorithm. When this occurs, the blockchain uses the largest ledger consensus mechanism to establish a common record of events.

The validators pick a block at random after a fork. Due to its unique qualities like immutability, auditability, and accountability, blockchain technology can enhance IoT by offering a platform for distributed blockchain information sharing. Participating nodes permanently record the transaction history on the blockchain, making the process highly auditable. Scalability, auditability, dependability, and security are just few of the areas where the distributed nature of cryptocurrencies might improve the Internet of Things [22].

### 3.2. Blockchain-based solutions

Due to its fundamental characteristics—anonymity, accessibility, trust lessness, and decentralization—blockchain technology has attracted a lot of interest as a viable solution to aid access control in IoT [23,24].

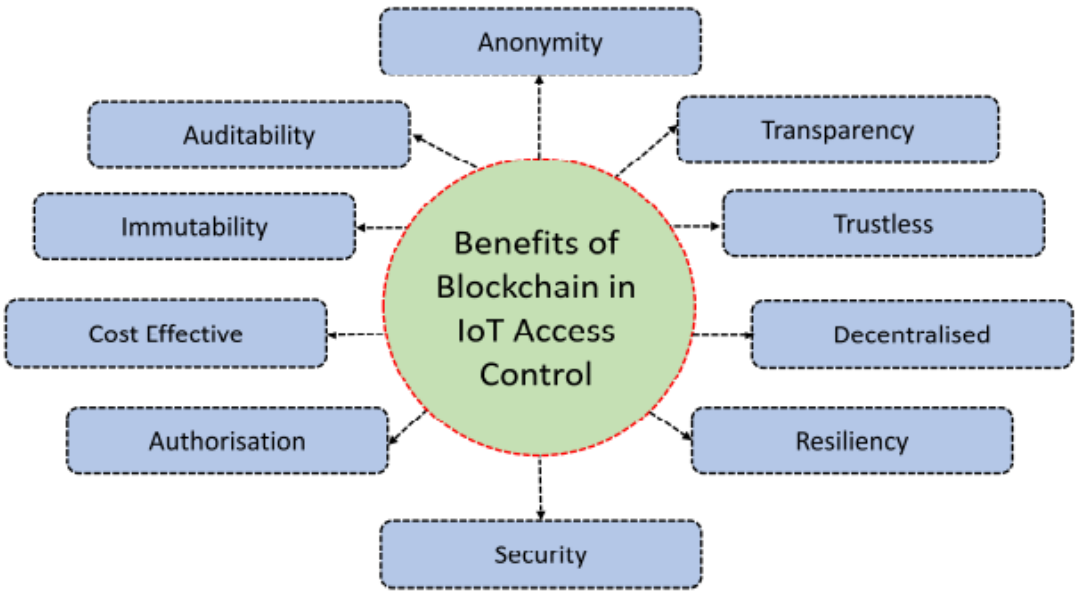


**Fig. 5. Several benefits of using blockchain for IoT access control [1]**



eISSN 1303-5150

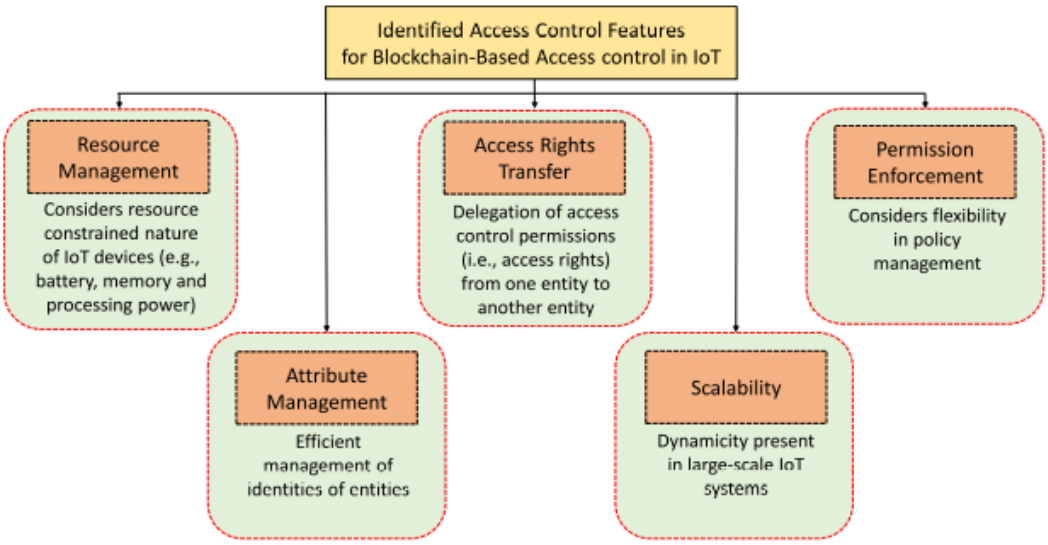


**Figure 6: illustrates the crucial access control components for Internet of Things solutions [1]**

To demonstrate these capabilities, we will use a made-up example of an Internet of Things-enabled smart house. As many IoT devices used in consumer devices are built to gather sensitive information, it is important that only authorized individuals have access to these systems and the information they create. Thanks to the anonymity provided by blockchain technology, homeowners may safely share their equipment with other people or robots. Token permissions can't be changed to increase privileges or other nefarious actions because of the blockchain's immutability, which makes access control systems more secure. In addition, smart property owners may always see a record of who has been granted and denied access to their gadgets and data because to the auditability provided by blockchain technology. along with the Internet of Things as a whole. Concise description of these qualities. In what follows, we'll look at five fundamentals of access control and the numerous cryptocurrency-based IoT access control solutions currently on the market.

The following five factors—good planning, the transfer of access permissions, the enforcement of approvals, the management of features, and scalability—are all ones that we place a high value on.

**3.2.1. Resource management**

As per IoT access control, there is a wide variety of possible interactions amongst smart devices when it comes to sharing and exchanging resources. The computational resources of an Internet of Things system must be efficiently organized, allocated, and shared. Users need safe and fast access to these assets so they may be put to good use, ideally in a decentralized setting. Resource management needs to account for the fact that IoT devices will have limited processing capacity for the foreseeable future. Blockchain might replace traditional centralized security methods for IoT data access, allowing for increased adaptability in the underlying resource management architecture. Keep in mind that in many situations with a large number of IoT., such as supply network, shipping, and gas, cryptocurrency lifts power from a centralized point and allows better flexibility in resource management [25].



eISSN 1303-5150

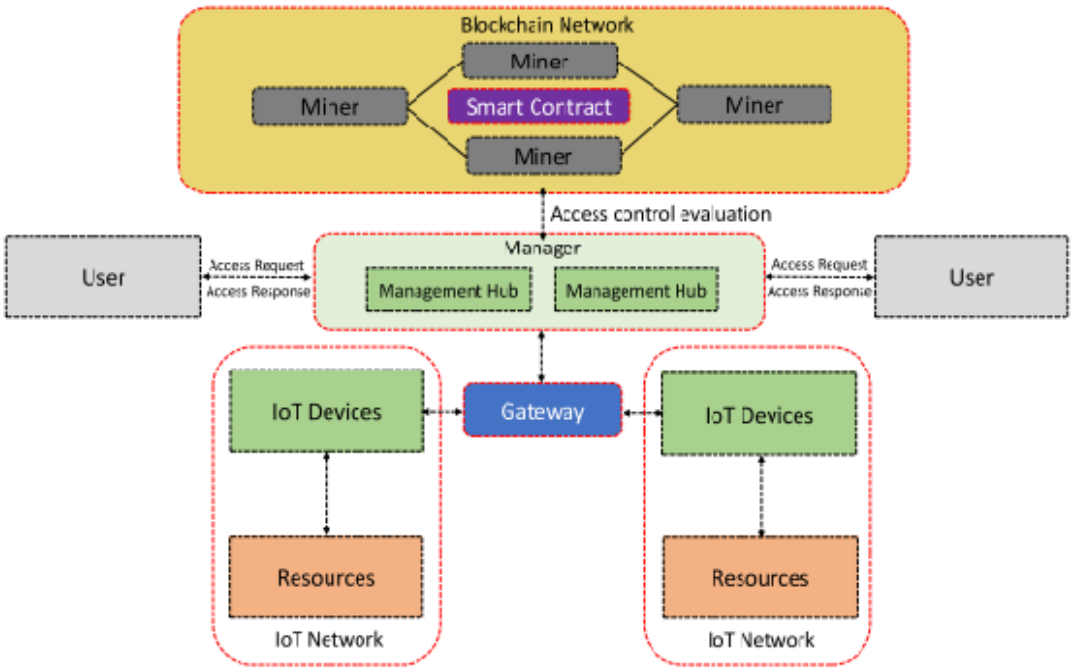


**Fig. 7. A blockchain-enabled access control architecture for IoT presented in Novo (2018) [1]**

This strategy uses a unified smart contract to simplify the whole blockchain network, cutting down on unnecessary communication between nodes and maximizing efficiency across the board. The authorized procedures are those that are listed in the smart contract. In this setup, IoT devices are not responsible for maintaining the blockchain network because of their low processing power. However, the architecture allows for edge IoT devices to communicate and pool resources with many IoT networks located in different parts of the world in real time. Centralized access-control systems are avoided and the challenges they cause are mitigated by implementing access policies that are mainly autonomous and take use of the bitcoin blockchain's strengths in efficient resource distribution. One or more managers are in charge of the management hubs and are also responsible for creating access permissions for the peripheral IoT devices. It's important to remember that the managers don't always have access to the bitcoin blockchain.

By making less use of the system's hardware, it greatly enhances its ability to manage its resources. Managers may assign private access control settings to individual edge devices for use at a certain point in time. A simple algorithm is included in the model to facilitate the rapid deployment of comparable Internet of Things devices. In a similar vein, the multi-agent-system-supported centralized models for access control presented in [26], [27], [28], and [29] show similar tendencies. To manage legitimate parties and enhance the management of available resources while cutting down on unnecessary traffic, Proposal employs a private tiered blockchain architecture. Data integrity is maintained by a validation agent, while entity authorization is checked by an authorization agent. With the use of a dual-blockchain (public and personal) platform idea, [27] and [28] verify entities based on the correct properties contained in the blockchain system.



eISSN 1303-5150

### 3.2.2. Access rights transfer

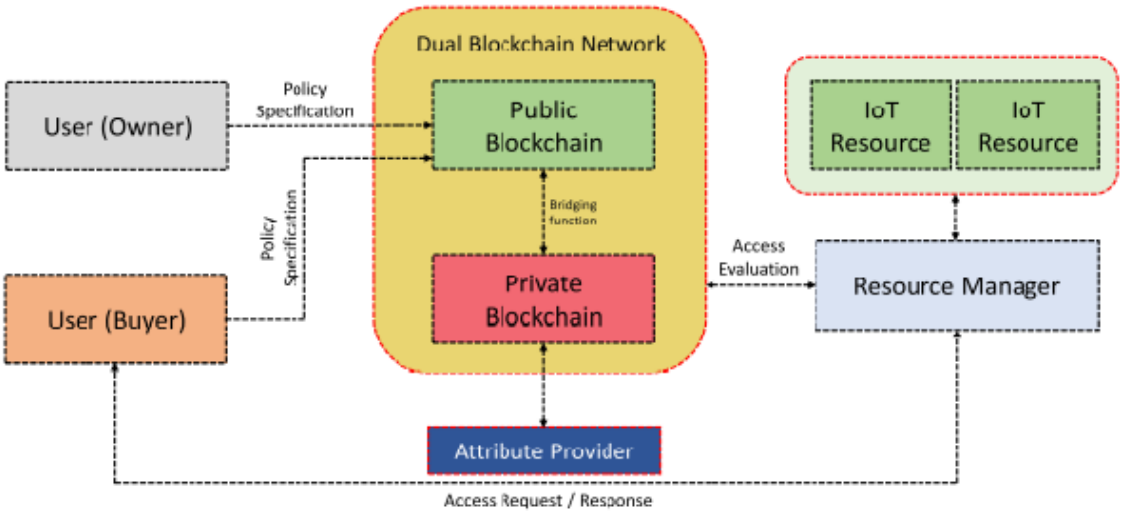


**Figure 8: An IoT access control architecture based on a dual-blockchain concept presented in Pal et al. (2020c) [1]**

Moving permissions from one object to another is essential for delegating fine-grained privileges. As an example, when a car requires fixing, the owner often gives the mechanic the go-ahead to perform whatever needs doing. Here, the customer authorizes the service center to fix their automobile using a computerized system (under a particular set of restrictions). Keep in mind that delegate is a method of transferring authorization [30]. Considering the significance of user password authentication for edge IoT devices, this has substantial implications for legal and policy settings. Integrate a private blockchain with the blockchain system to create a "dual-blockchain" platform, refining their strategy for a bitcoin access control platform (cf. Fig. 8).

Users' privacy is better protected when sensitive features are stored in an input provider overseen by the private blockchain. This becomes more vital as the scope and complexity of an Internet of Things system expand. To simplify the transfer of access privileges across IoT devices, bitcoin events are used as attributes (also known as privilege or access tokens) instead of [31]. A trustworthy third party is unnecessary for the desired functioning of a smart contract. An online business model is used to discuss the solutions' potential usefulness (owner and buyer are involved). The rollout is comprehensive.

### 3.2.3. Permission enforcement

The proper access control permissions for a large number of geographically scattered IoT devices involve collaboration at the edge of the network. The versatility and longevity of blockchain technology make it a good fit for various uses. It is in very complicated situations when documents are used to verify and enforce rights [32]. In addition, blockchain may be used to impose granular limits on who has access to which shared resources.

This allows for a lightweight and decentralized access control system to make use of smart contracts to enforce permissions. The proposed approach aims to enable trustworthy access controls and secure messaging with edge IoT devices, and it is defined by the intrinsic properties of the underlying blockchain, such as scalability, data integrity, and visibility. Private cryptocurrencies sometimes utilize a hierarchical structure to regulate



eISSN 1303-5150

access to their network (e.g., at the user level and blockchain level). Block creation on the blockchain can be slowed down by validators by temporarily pausing the LSB's lightweight consensus process. Implementing reliable access-control measures Through the development of mutual trust, the quantity of computational resources required to validate both blocks and transactions may be reduced. The blockchain's capacity to handle self-scaling features is guaranteed via a shared capacity control mechanism, and trust is established by looking at nodes' past actions.

**3.2.4. Attribute management**

Decentralized, adaptable, and fine-grained IoT device authentication relies heavily on attribute management. Because a target can utilize attributes to specify granular access laws, they're crucial for determining whether or not the requesting entity has the necessary authorizations.



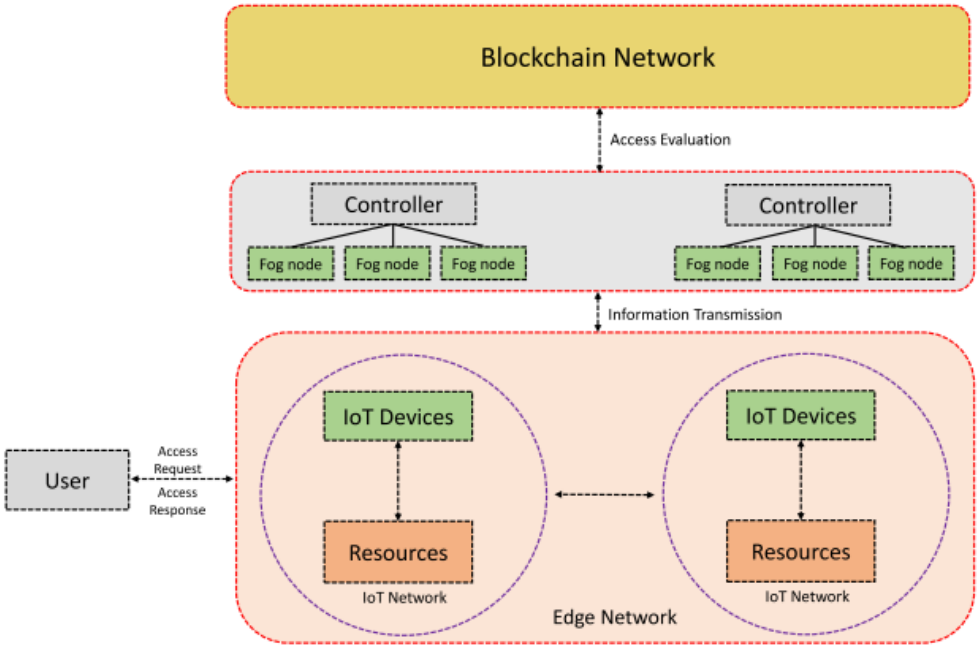


**Fig. 9. Fog computing for IoT access control in blockchain-based solutions [1]**

In addition, this concept offers a decentralized, lightweight method of access control, wherein all that is needed for IoT devices to carry out an authorization task is a chain of access data. In addition, it is important to note that the proposals [33] rely on characteristics rather than entities' unique concrete identities to validate them. When an entity does not want to share or distribute its unique identity with any other entities, this authorization procedure can be used.

**3.2.5. Scalability**

There has been a recent uptick in research on blockchain's potential for use in IoT access control [34], specifically in relation to how it may be integrated with emerging fog technology applications. Figure 9 shows how fog computing might be employed in blockchain-based systems for IoT access management. Always keep in mind that blockchain is a distributed ledger that may be used to access data safely since it is not centralized. Towards the goal of distributed authorization in the Internet of Things, this helps. To better aggregate, manage, and analyze massive volumes of data transfer and workload for Internet of Things (IoT) devices, cloud computing technology has included fog-based architecture. In a fog-based architecture, the fog nodes that sit across edge devices and the cloud

servers are located as near to the edge device as practicable.

This provides for finer-grained control over who in the network has access to what kinds of data. Each controller also has its own special set of safeguards against potential security breaches. The system's scalable distribution of computational power and storage capacity reduces administrative and processing overheads.

**4. Discussions**

Several approaches deal with the pressing issue of developing access control methods that are specifically suited to IoT systems, taking into account their requirements and contexts. These ideas also noted the need for dedicated hardware and software to fully capture the nuances of IoT access control, such as how it should be implemented and policed.

To guarantee safe, efficient, and trustworthy network connectivity for the Internet of Things (IoT) in the future, a number of unanswered questions must be answered first. What follows are only a few of instances in point:

**4.1. Policy management**

It's not easy to tell who's who among the numerous people, machines, and gadgets that make up an IoT device. In addition, strong policy administration is essential for restricting access to system resources for only approved users. Policy enforcement and user access to internal system data must be included in from the start. Moreover, how the instruments must carry out autonomous authorization in tandem [35]. We propose that this may be achieved by simultaneously recognizing the access control needs and implementing a minimum set of access restrictions on edge IoT systems. However, this part of policy decision making is challenging to accomplish utilizing the edge intelligence of IoT devices.

To what extent can access polices for the IoT be managed at scale without the intervention of a central authority is a key research topic in this area. As a result, the bitcoin blockchain becomes a more viable option for decentralized authorization and policy administration. A policy control mechanism for blockchain is needed to properly represent access rights and guarantee the global transfer of those rights across organizations. On addition, the policy quality audit is transformed into exactable smart contracts when dealing with access control guidelines in blockchain, which provides additional security features like verifiability, auditability, and data integrity.



**4.2. Trust management**

Traditional trust management strategies for information and resource sharing between entities might be ineffective in an IoT system because of its scale and heterogeneity [36]. Yet it is challenging to manage trust in an IoT system. Variability and high system dynamics compound the challenge of building a trustworthy environment in the IoT and highlight the need for better trust mechanisms. Context-dependent, subjective, and influenced by social factors, trust and the accompanying access control permissions must be measured. IoT adds another layer of complexity since the context can shift rapidly based on the surrounding environment.

Uncertainty is a major obstacle when working with decentralized networks like multi-agent systems, in which autonomous entities (like agents) must carry out certain tasks either independently or on request of a human user. That is to say, how to display trust in both natural and manufactured uncertainties is a major open question in the field because of the positive aspects of trust (such as its dynamic, informational, recursive, etc. nature) and the many sources of uncertainty. The outcome of a transaction is an example of natural uncertainty, while artificial doubt is the effect of hearing something secondhand (i.e., viewpoints obtained from other people, places, or things).

**4.3. Standardization**

Connection and standards within devices, apps, and services can be challenging to handle due to the nature of IoT. The Internet of Things makes



eISSN 1303-5150

use of a wide variety of protocols. Low-power Wi-Fi, RFID, NFC, Sigfox, 6LoWPAN (Low-Power Wireless Personal Area Networks Networks), Lora WAN, and many more are only some of the communication protocols used by the IoT stack. Lightweight protocols given by IETF standards and software update methods like MQTT (Message Queuing Telemetry Transport) and CoAP are also helpful for resource-constrained IoT devices (Constrained Application Protocol). If gadgets don't communicate with each other, no information can be shared between them (via standardized protocols). Lightweight protocols are necessary for trustworthy and secure data transfer on the one hand because of the constraints placed on IoT devices in terms of ram, battery life, or computing capability. Data security for all of the Devices in the network and the IoT as a whole is a major concern if an appropriate protocol is not in place to secure the data during transmission and storage.

**4.4. Identity management**

To insist that every transaction in an IoT setting must be completely unique seems too stringent to us. It may be essential in certain circumstances, but in others, restricted identities will suffice to meet the demands of software products and policy standards. It's possible that we'd do this if we were dealing with a small number of smart home products, giving each one a distinct name. However, due to the complexity and number of possible weak points in an IoT-enabled manufacturing logistics network, identification restrictions are essential.

Detailed and extensive investigation, assessment, and categorization are required to examine the appropriateness of various identity strategies inside this environment of an IoT system [37]. Though several identity management paradigms have been offered, none have yet proven themselves capable of discussing the scale and diverse nature of IoT systems. Blockchain technology can help build robust network meshes that keep IoT devices' identities private as they securely exchange data. Implementing efficient consensus mechanisms will allow for this to happen.

As a uniform, reusable, and tamper-proof infrastructure, cryptocurrencies are a promising platform that may be able to solve the scalability problems associated with IoT identification difficulties. This changes the identity management system to one that is less centrally controlled. Furthermore, smart contracts can provide the "trusted" auditability necessary for IoT access control systems, allowing for the controlled disclosure of data.



**5. Future research directions**

Our research revealed a pressing requirement for proper access control methods to be put in place to protect Internet of Things devices from hackers and other malicious actors. Lightweight, flexible, and tightly regulated access control techniques that may be tailored to the specific needs of an IoT system are required (such as dynamic, large-scale, and so on). Therefore, in the future, there will be a need for comprehensive study for IoT trust management, in addition to the access control requirements and design standards that enable improved permissions enforcement brought about by the technology. Protecting the technologies and infrastructures that bridge the digital and physical realms is an important goal of the Internet of Things (IoT), and blockchain integration into access control can contribute to this goal. There is more leeway to access these rules whenever they are needed thanks to the blockchain's encoded and secure storage of access control processes within the blocks, which also increases data security and reliability.

The risks related to a particular access control system that would be present in such highly dynamic IoT systems, as well as the design and creation of advanced agents with better overall capabilities to regulate blockchain, present some of the largest barriers for ML adaptation in blockchain in IoT. Combining ML-assisted data fusion techniques

for multilayer, middleware bitcoin systems for data authorization in IoT requires the development of an efficient access control framework. The use of machine learning algorithms in smart contracts may also play a role. It calls for creative responses from the academic and professional communities.

**6. Conclusions**

As the Internet of Things (IoT) continues to expand at a breakneck pace, research into the IoT has become and will continue to be an urgent matter. Internet of Things (IoT) security is a major issue. Safe access management is an important factor. We have observed that conventional means of maintaining access controls and enforcing authorization decisions are inadequate in the context of large-scale IoT networks. However, a specialized method of security must be implemented for IoT networks. We found that the blockchain can provide the tamper-proofness, data openness, and auditability needed for effective IoT access management. The existing IoT physical access surveys have a widespread problem: they don't pay enough attention to the advancement of blockchain technology. In this post, we looked at how blockchain technology is currently being used to secure the Internet of Things. By classifying existing blockchain-based access control solutions for the IoT according to the specific access requirement they meet, like handling resources, user account transfer, written consent enforcement, descriptor management, and scalability, we provided a comprehensive discourse of these solutions. We have demonstrated that blockchain, in contrast to conventional access control systems, may be used to overcome the limitations of controlling IoT connection. Our analysis also included many key areas for further study, including identity verification, trust, and policy, with the ultimate goal of delivering blockchain-enabled Internet of Things (IoT) networks that are adaptable, decentralized, trustworthy, and functional.

**REFERENCES**

[1] Shantanu Pal, Ali Dorri, Raja Jurdak, Blockchain for IoT access control: Recent trends and future research directions, Journal of Network and Computer Applications, Volume 203,2022,103371, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2022.103371.

[2] Anon, 2021b. Cisco: The zettabyte era: Trends and analysis. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni_hyperconnectivity-wp.html. [Online: Accessed 24-Oct-2021].

[3] Andaloussi, Y., Ouadghiri, M., Maurel, Y., Bonnin, J., Chaoui, H., 2018. Access control in iot environments: Feasible scenarios. In: The 9th International Conference on Am_bient Systems, Networks and Technologies. Procedia Comput. Sci. 130, 1031–1036, URL http://www.sciencedirect.com/science/article/pii/S1877050918305064.

[4] Tolone, W., Ahn, G., Pai, T., Hong, S., 2005. Access control in collaborative systems. ACM Comput. Surv. 37 (1), 29–41. http://dx.doi.org/10.1145/1057977.1057979.

[5] Uganya, G., Radhika, Vijayaraj, N., 2021. A survey on internet of things: Applications, recent issues, attacks, and security mechanisms. J. Circuits Syst. Comput. 30 (05), http://dx.doi.org/10.1142/S0218126621300063.

[6] Pal, S., 2021. Internet of Things and Access Control: Sensing, Monitoring and Con_trolling Access in IoT-Enabled Healthcare Systems, vol. 37. Springer Nature, http://dx.doi.org/10.1007/978-3-030-64998-2.

[7] Dramé-Maigné, S., Laurent, M., Castillo, L., Ganem, H., 2021. Centralized, distributed, and everything in between: Reviewing access control solutions for the IoT. ACM Comput. Surv. 54 (7), 1–34. http://dx.doi.org/10.1145/3465170.

[8] Pal, S., Hitchens, M., Varadharajan, V., Rabehaja, T., 2019a. Policy-based access control for constrained healthcare resources in the context of the internet of things. J. Netw. Comput. Appl. 139, 57–74. http://dx.doi.org/10.1016/j.jnca.2019.04.013.

[9] Majeed, U., Khan, L., Yaqoob, I., Kazmi, S., Salah, K., Hong, C., 2021. Blockchain for IoT-based smart cities: recent advances, requirements, and future challenges. J.Netw. Comput. Appl. 181, http://dx.doi.org/10.1016/j.jnca.2021.103007.

[10] Wang, X., Zha, X., Ni, W., Liu, R., Guo, Y., Niu, X., Zheng, K., 2019a. Survey on blockchain for internet of things. Comput. Commun. 136, 10–29. http://dx.doi.org/10.1016/j.comcom.2019.01.006.

[11] Dukkipati, C., Zhang, Y., Cheng, L., 2018. Decentralized, blockchain based access control framework for the heterogeneous internet of things. In: Third ACM Workshop on Attribute Based Access Control. ABAC'18, New York, USA, pp. 61–69. http://dx.doi.org/10.1145/3180457.3180458.

[12] Jameel, F., Hamid, Z., Jabeen, F., Zeadally, S., Javed, M., 2018. A survey of device_to-device communications: Research issues and challenges. IEEE Commun. Surv. Tutor. 20 (3), 2133–2168. http://dx.doi.org/10.1109/COMST.2018.2828120.

[13] Ashton, K., 2009. That 'Internet of Things' Thing. RFID J. http://www.rfidjournal.com/articles/view?4986.

[14] Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R., Ni, W., 2018. Anatomy of threats to the internet of things. IEEE Commun. Surv. Tutor. http://dx.doi.org/10.1109/COMST.2018.2874978.

[15] Butun, I., Österberg, P., Song, H., 2020. Security of the internet of things: Vulnerabil_ities, attacks, and countermeasures. IEEE Commun. Surv. Tutor. 22 (1), 616–644. http://dx.doi.org/10.1109/COMST.2019.2953364.

[16] Patel, C., Doshi, N., 2019. Security Challenges in IoT Cyber World. Springer Inter_national Publishing, Cham, pp. 171–191. http://dx.doi.org/10.1007/978-3-030-01560-2_8.

[17] WIRED, 2020. How the Internet of Things got Hacked. https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/, [Online: Accessed 01-Oct-2020].

[18] Anon, 2020a. Mirai botnet ddos attack type. https://www.corero.com/resources/ddos_attack-types/mirai-botnet-ddos-attack.html/, [Online: Accessed 10-Oct-2020].

[19] Anon, 2020b. The Internet of Things: Cayla doll is banned in Germany over privacy and security concerns.

[20] Robinson, S., 2019. Smart home attacks are a reality, even as the smart home market soars. https://www.cisco.com/c/en/us/solutions/internet-of-things/smarthome-attacks.html [Online: Accessed 25-May-2019].

[21] Xu, R., Chen, Y., Blasch, E., 2020. Decentralized access control for IoT based on blockchain and smart contract. Model. Des. Secure Internet of Things 505–528. http://dx.doi.org/10.1002/9781119593386.ch22.

[22] Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H., 2017. An overview of blockchain technology: Architecture, consensus, and future trends. In: IEEE International Congress on Big Data (BigData Congress). pp. 557–564. http://dx.doi.org/10.1109/BigDataCongress.2017.85.

[23] Conoscenti, M., Vetrò, A., Martin, J., 2016. Blockchain for the internet of things: A systematic literature review. In: IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). pp. 1–6. http://dx.doi.org/10.1109/AICCSA.2016.7945805.

[24] Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R., Michelin, R., Zorzo, A., Kanhere, S.,2020. Blockchain technologies for IoT. In: Advanced Applications of Blockchain Technology. Springer, pp. 55–89. http://dx.doi.org/10.1007/978-981-13-8775-3_3.

[25] Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M., 2018. On blockchain and its integration with IoT. challenges and opportunities. Future Gener. Comput. Syst. 88, 173–190. http://dx.doi.org/10.1016/j.future.2018.05.046.

[26] Chen, W., Xu, Z., Shi, S., Zhao, Y., Zhao, J., 2018. A survey of blockchain applications in different domains. In: The International Conference on Blockchain Technology and Application. pp. 17–21. http://dx.doi.org/10.1145/3301403.3301407.

[27] Chen, W., Xu, Z., Shi, S., Zhao, Y., Zhao, J., 2018. A survey of blockchain applications in different domains. In: The International Conference on Blockchain Technology and Application. pp. 17–21. http://dx.doi.org/10.1145/3301403.3301407.

[28] Pal, S., Rabehaja, T., Hitchens, M., Varadharajan, V., Hill, A., 2020c. On the design of a flexible delegation model for the internet of things using blockchain. IEEE Trans. Ind. Inf. 16 (5), 3521–3530. http://dx.doi.org/10.1109/TII.2019.2925898.

[29] Pal, S., Rabehaja, T., Hill, A., Hitchens, M., Varadharajan, V., 2020b. On the integration of blockchain to the internet of things for enabling access right delegation. IEEE Internet Things J. 7 (4), 2630–2639. http://dx.doi.org/10.1109/JIOT.2019.2952141.

[30] Algarni, S., Eassa, F., Almarhabi, K., Almalaise, A., Albassam, E., Alsubhi, K., Yamin, M., 2021. Blockchain-based secured access control in an IoT system. Appl. Sci. 11 (4), http://dx.doi.org/10.3390/app11041772.

[31] Rabehaja, T., Pal, S., Hitchens, M., 2019. Design and implementation of a secure and flexible access-right delegation for resource constrained environments. Future Gener. Comput. Syst. 99, 593–608. http://dx.doi.org/10.1016/j.future.2019.04.035.

[32] Le, T., Mutka, M., 2018. Capchain: A privacy preserving access control framework based on blockchain for pervasive environments. In: IEEE International Confer_ence on Smart Computing (SMARTCOMP). pp. 57–64. http://dx.doi.org/10.1109/SMARTCOMP.2018.00074.

[33] Unal, D., Hammoudeh, M., Kiraz, M., 2020. Policy specification and verification for blockchain and smart contracts in 5g networks. ICT Express 6 (1), 43–47. http://dx.doi.org/10.1016/j.icte.2019.07.002.

[34] Pal, S., Rabehaja, T., Hitchens, M., Varadharajan, V., Hill, A., 2020c. On the design of a flexible delegation model for the internet of things using blockchain. IEEE Trans. Ind. Inf. 16 (5), 3521–3530. http://dx.doi.org/10.1109/TII.2019.2925898.

[35] Kiwelekar, A., Patil, P., Netak, L., Waikar, S., 2021. Blockchain-Based Security Services for Fog Computing. Springer International Publishing, Cham, pp. 271–290. http://dx.doi.org/10.1007/978-3-030-57328-7_11.

[36] Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., Fang, B., 2020b. A survey on access control in the age of internet of things. IEEE Internet Things J. 7 (6),





eISSN 1303-5150

4682–4696. http://dx.doi.org/10.1109/JIOT.2020.2969326.

[37] Sharma, A., Pilli, E., Mazumdar, A., Gera, P., 2020. Towards trustworthy internet of things: A survey on trust management applications and schemes. Comput. Commun. 160, 475–493. http://dx.doi.org/10.1016/j.comcom.2020.06.030.

[38] Mahalle, P., Babar, S., Prasad, N., Prasad, R., 2010. Identity management framework towards internet of things (IoT): Roadmap and key challenges. In: International Conference on Network Security and Applications. Springer, pp. 430–439. http://dx.doi.org/10.1007/978-3-642-14478-3_43.