Review

Authentication and Access Control Mechanisms to Secure IoT Environments: A comprehensive SLR

Seetah Almarri * and Mounir Frikha

Posted Date: 14 May 2024

doi: 10.20944/preprints202405.0948.v1

Keywords: IoT; access control; authentication; attribute-based access control; role-based access control

 doi:10.20944/preprints202405.0948.v1

Review

Authentication and Access Control Mechanisms to Secure IoT Environments: A Comprehensive SLR

Seetah Almarri * and Mounir Frikha

Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia; mmfrikha@kfu.edu.sa

* Correspondence: 224108483@student.kfu.edu.sa

Abstract: Due to the rapid growth of the Internet of Things (IoT), securing communications between a huge number of devices has become very difficult. Access controls and authentication secure the connection between IoT devices and protect sensitive data from unauthorized users or malicious attackers. In this paper, we provide a comprehensive review to emphasize the critical role of authentication and access control in securing IoT environments. This paper explores different types of access controls, like Attribute-Based Access Control and Role-Based Access Control. Furthermore, it demonstrates different authentication techniques, like passwords and biometrics. Based on the previous mechanisms, we discuss different IoT security challenges regarding authentication and access control mechanisms and highlight future directions. In addition, this paper investigates the integration between access control and authentication to safeguard IoT communications.

Keywords: IoT; access control; authentication; attribute-based access control; role-based access control

1. Introduction

The Internet of Things (IoT) has expanded in recent years, changing numerous industries and creating new possibilities for innovative applications. IoT devices are connected together to enable data sharing and facilitate communications. They might be anything from industrial sensors to smart household appliances. But this connectivity also may cause serious security risks, especially when it comes to safe authentication and access control. For IoT ecosystems to remain secure overall, data integrity and confidentiality must be guaranteed for both data sent and received by IoT devices.

Networks and IoT devices need to be protected from malicious activity and malicious access through the use of secure access control and authentication techniques. IoT environments have specific security requirements that are frequently bypassed by traditional authentication techniques like usernames and passwords. Specialized access control and authentication solutions are required because of the resource limitations and diverse architectures of IoT devices.

As a result, a lot of research has gone into investigating and improving the security of IoT systems using innovative access control and authentication techniques. Establishing the identity of IoT devices, authenticating users or entities engaging with them, and enforcing access controls to safeguard sensitive information and assets are the goals of these techniques.

The contribution of this paper is as follows:

1. Determining and analyzing the research papers that have already been written about access control and secure authentication in IoT communications.
2. Delving into the several authentications and access control techniques that have been suggested for IoT communications.
3. Listing all challenges and open research issues about authentication and access control to secure IoT.
4. Offering analysis and recommendations for research future directions.

Our goal is to provide a novel knowledge of the state-of-the-art in secure authentication and IoT-related access control. Researchers interested in IoT security will find the review's conclusions to be beneficial, as they will help them to make informed decisions and create practical solutions to the security issues raised by IoT.

 doi:10.20944/preprints202405.0948.v1

This paper is structured as follows: Section 2 shows the methodology used to organize this paper. Section 3 provides an overview of IoT authentication mechanisms. Section 4 presents an overview of IoT access control mechanisms. Section 5 explores the state-of-the-art studies in this field. Section 6 determines the challenges and future directions of IoT security authentication and access control. Finally, Section 7 concludes the paper by summarizing the key findings.

1.1. Motivations

Access control and authentication systems are becoming more and more sophisticated, and this makes a thorough understanding of them necessary to ensure safe IoT connections. In order to solve the issues surrounding IoT security, this study seeks to analyze current research, determine practical solutions, and address IoT security challenges.

Moreover, authentication and access control face specific challenges due to the variety of IoT devices and communication protocols. To do that, we will investigate a range of methods, from well-known ones like username/password authentication to more innovative ones like biometric-based authentication and Multi-Factor Authentication (MFA).

Another important aspect of IoT security is data privacy because IoT devices gather and transfer a lot of sensitive data. We will find privacy-enhancing authentication and access control solutions that help organizations to meet requirements for data protection and user privacy concerns by reviewing this paper.

1.2. Scope

This paper's scope includes the following:

- The study looks at a number of authentication techniques suggested for IoT environments, such as MFA, certificate-based authentication, biometric authentication, and the conventional username/password method.
- Various access control mechanisms that apply to IoT environments are examined in this study. Context-aware access control, Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC) are examples. In the analysis, we will examine their suitability , scalability and effectiveness for various IoT applications.
- The paper examines the special qualities and limitations of IoT devices, including their constrained amounts of memory, processing power, and energy. It looks at how these restrictions affect the way secure authentication and access control systems are designed and implemented for the IoT and looks into effective, low-cost solutions that can work around these restrictions.
- The paper explores the security concerns that raise from authentication and access control in the IoT. These challenges include those relating to scalability, privacy, interoperability, and standardization. It examines the developments and fixes to deal with these issues and tries to minimize security threats in IoT environments.

2. Papers Selection for Literature Review

2.1. Methodology

The methodology used in this research is a systematic literature review (SLR). SLR is used to present the information in a clear and organized way. Also, it will help in identifying the limitations and the research gaps that exist in current studies. In addition, it will help in the determination of the research's future direction. Furthermore, PRISMA flow diagram was used to summarize steps that were followed by researchers during the paper selection process. Identification, screening, and inclusion are the main phases that were followed in the PRISMA flow diagram. In addition, the research targeted the studies that were published between 2020 and 2024. In the identification phase, duplicated and ineligible records were removed after filtering the year and source type, whether journal, book, or conference. In the screening phase, additional records were excluded for other

 doi:10.20944/preprints202405.0948.v1

reasons, like relevance to the research topic or the length of the paper. Finally, the included phase will contain only the papers that will be included in the research.

2.2. Search String

The following search string was used to optimize the quality of the search results: ("Authentication" OR "Access control") AND ("IoT") AND ("Secure" OR "security") AND ("Communications"). It consists of Boolean operators like "AND" and "OR" between the key words. These operators will greatly help in broadening, narrowing and adjusting the search string.

2.3. Data Sources

The search string was applied in two databases which are Google Scholar and Saudi Digital Library.

2.4. Screening Process

In the first stage, we filtered the papers based on their titles by searching the database using a search string, looking if the title was related to our topic or not. If there are some difficulties in evaluating the paper topic, we added an extra screening stage which is by reading the abstract of that paper. Figure 1 shows the PRISMA flow diagram, which presents the selection process of the papers.

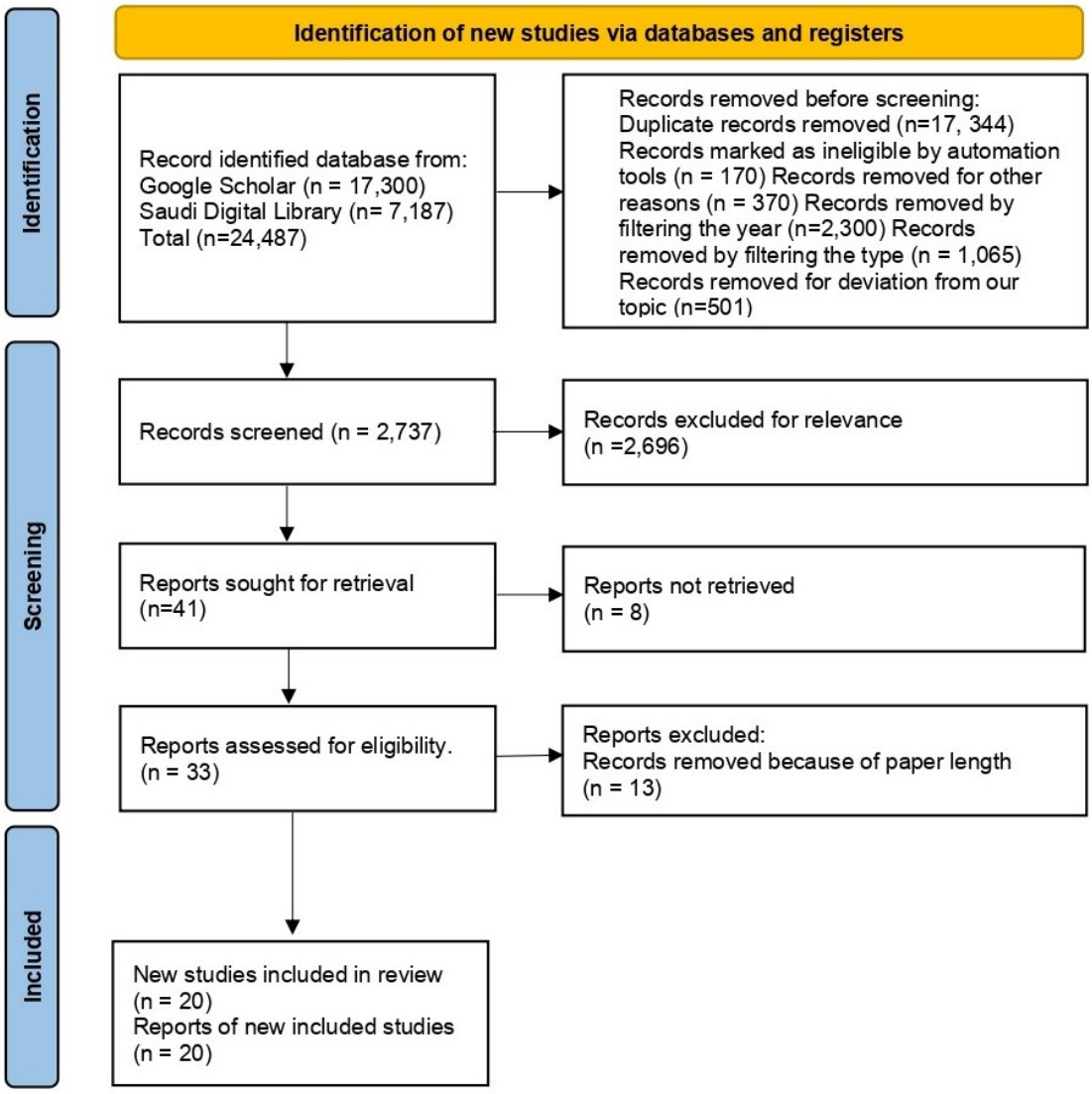

Figure 1. Papers selection for literature review using PRISMA.

 doi:10.20944/preprints202405.0948.v1

2.5. Data charting process

All charts in this paper are charted by LucidChart. https://www.lucidchart.com

2.6. Systematic Review registration statement

A thorough and open systematic review requires the use of a registration statement for the systematic review. In order to ensure transparency and reduce the possibility of bias in the review process, it gives a thorough explanation of the goals, procedures, and anticipated analysis of the review. The Open Science Framework (OSF) is used in this paper for registering systematic reviews. https://osf.io/28snc/

3. Overview of IoT Authentication Mechanisms

IoT authentication techniques are a fast-growing field that aims to handle the special difficulties and security risks that come with IoT networks. In his thorough review of hardware- and software-based authentication methods for the Internet of Drones, Michailidis [1] emphasizes the necessity of lightweight solutions because of resource limitations. Mehta [2] addresses the difficulties and risks associated with IoT network authentication while highlighting its significance, especially in light of security and protection considerations. In addition, data security in IoT is a crucial concern, particularly in terms of authentication and access control. Authentication techniques are important to secure IoT devices and communications against unauthorized access or cyberattacks. Also, authentication is a primary stage to ensure that only authorized users, entities, and devices can access certain data. Furthermore, authentication mechanisms aim to determine and remove suspicious nodes from IoT networks [3]. In this section, different authentication techniques that are applicable in IoT are explored.

- **Password-based authentication:** Passwords are the most common authentication method. Devices in IoT environments use a combination of username and password to authenticate other devices. Using only passwords is not enough to provide optimum security, especially when weak passwords are used. Also, brute-force attacks can be used to guess the passwords.

  Both Hammi [4] and Alshahrani [5] offer creative password-based authentication methods for the IoT. Alphanumeric and graphical passwords are combined in Alshahrani's graphical-based password scheme, IoT-GP, a two-factor technique that greatly enhances security and usability. With excellent security and performance, Hammi's lightweight ECC-based authentication technique uses isogeny and Elliptic Curve Cryptography (ECC) to expand on the One-Time Password (OTP) concept. In order to defend against dictionary and brute force attacks, Tarish [6] recommends using the Secure Remote Password Protocol (SRPP) in Wi-Fi-based IoT networks.
- **Public Key Infrastructure (PKI):** This type of authentication depends on the cryptography keys, involving both public and private keys. Every device in IoT environments has a unique private key, while the public key remains for the public to be used by other servers or other devices.

  A lightweight certificate enrollment mechanism and a profile for X.509 digital certificates are introduced by Höglund [7] in order to meet the resource limitations of IoT devices. In order to improve storage, communication, reaction time, and resistance against malicious nodes, Belattaf [8] offers a distributed public-key management infrastructure that is both dependable and adaptable. Using a different strategy, Antony [9] proposes a blockchain-based PKI that provides safe data sharing for IoT-based healthcare systems. Balakrichenan [10] investigates the creation of a PKI for the IoT by utilizing the Domain Name System (DNS) infrastructure, especially the DNS-based Authentication of Named Entities protocol (DANE) and DNS's Security Extensions (DNSSEC).
- **X.509 certificates:** Digital papers called X.509 certificates link an identity to a public key. When establishing their identity with other devices or servers, IoT devices can employ X.509 certificates. The device's validity and integrity can be confirmed by relying parties through the verification of certificates that are provided by a reliable Certificate Authority (CA).

 doi:10.20944/preprints202405.0948.v1

Using X.509 certification and LZW compression, Karthikeyan [11] suggests a way for data security in IoT networks. Höglund [7] concentrates on addressing the resource limitations of IoT devices through the creation of a lightweight certificate enrollment protocol and an X.509 digital certificate profile known as XIOT. A blockchain-based lightweight certificate authentication solution that does not rely on Certification Authorities is introduced by Garba [12] as LightCert4IoT. L-ECQV is a lightweight ECQV implicit certificate that minimizes message overhead and energy usage for IoT authentication, as presented by Malik [13].

- **OAuth and OAuth 2.0:** Widely employed in IoT applications, OAuth is an authorization protocol that permits safe resource access on behalf of a user or device. By using OAuth, a third-party service or application (referred to as the OAuth provider) can grant access to resources without disclosing the user's credentials. This is known as delegated permission. Widely used for IoT installations, OAuth 2.0 is an enhanced version of the protocol.

  This is further improved by the ACE-OAuth framework, which extends OAuth 2.0 to accommodate IoT device restrictions and incorporates CoAP [14]. OAuth 2.0 is suggested as a useful option for authorization and authentication in certain applications, such as Forestry 4.0 [15]. Oh et al. [16] highlight the necessity of security interoperability in diverse IoT platforms and suggest the interoperable OAuth 2.0 framework as a potential solution.
- **Token-based authentication:** Every authorized entity in the IoT network has a unique token that will be used for other authentication requests rather than the need to send credentials information with every request. In addition, the tokens can be live shortly, revocable, and tied to specific permissions to improve the scalability and security of IoT environments.

  In order to provide safe and decentralized identity management, several studies have suggested token-based authentication methods for the IoT [17]. These protocols make use of blockchain technology and fog computing. The use of Ethereum smart contracts for secure connectivity between miner nodes and IoT devices [18] and random forest learning for authorization and key management [19] are two further elements that have improved these protocols. The security and functionality of token-based authentication in the IoT have greatly enhanced as a result of these developments.
- **Mutual authentication:** The server and gateway have to authenticate each other before starting the connection, which prevents unauthorized access or special types of attacks like Man-In-The-Middle (MITM) from accessing the IoT network.

  Simplicity, optimality, and efficiency have been prioritized in the exploration of various techniques and algorithms for mutual authentication in IoT devices [20]. To solve security weaknesses, especially in RFID-based IoT systems, an effective authentication strategy based on mutual key update and self-adaptation has been presented [21]. With an emphasis on efficiency and simplicity, attribute-based encryption has been used to construct private and mutual authentication protocols that safeguard the privacy of IoT devices [22].
- **Biometric authentication:** Biometric authentication uses biometric individual information to authenticate users who are using IoT devices. Every individual has unique biometric information, such as facial recognition, fingerprints, and voices.

  Secure biometric authentication solutions for IoT devices are proposed by Golec [23] and Bedari [24], with Golec concentrating on edge devices and Bedari on industrial IoT devices over 5G networks. Both studies stress the significance of safe data transmission and storage; Golec emphasizes the use of AES-128-bit key encryption, while Bedari presents a fingerprint template that can be cancelled. While Rao [25] introduces a user authentication protocol for IoT networks, highlighting the necessity of dual-factor authentication and strong encryption, Alsellami [26] gives an overview of the possibilities of biometric authentication in IoT. The combined findings of these studies highlight how biometric authentication can improve the security and privacy of IoT devices.

 doi:10.20944/preprints202405.0948.v1

- **Multi-Factor Authentication (MFA):** MFA is the combination of two authentication methods like passwords, biometrics, tokens or smart cards. MFA enhances security by adding an extra layer of protection against unauthorized access to IoT devices.

  Mishra [27] proposes an MFA-integrated cloud-based security system for Industry 4.0 communication. With an emphasis on identity, password, and digital signatures, Saqib [28] presents a framework for lightweight three-factor authentication for essential IoT applications. An improved IoT security architecture for authorization and authentication, which includes MFA, is presented by Al-Refai [29] to fend against various sorts of threats. With the goal of enhancing efficiency and resource management, Sudha [30] suggests a low-area design of two-factor authentication utilizing the substitution-box-based inverter and Data Inverting Encoding Scheme (DIES) for IoT security.

4. Overview of IoT Access Control Mechanisms

Access control techniques are essential for protecting IoT devices and communications because they manage which users can access what resources and under what circumstances. By limiting unauthorized access, data breaches, and malicious activity, these techniques ensure that only authorized entities can connect with and use IoT devices. In this section, we explore different access control mechanisms that can be applied to secure the IoT.

- **Authorization:** Authorization guarantees that only authorized entities can access specific resources or functionalities. Authorization defines the actions that authenticated users or devices are allowed to perform and is based on roles, permissions, or attributes. For instance, some users may have limited access to IoT data, while others have full access to devices.

  The constraints of conventional access control methods are addressed by Putra [31] and Hameed [32] with their proposals for blockchain-based authorization mechanisms for IoT. Using Attribute-Based Access Control (ABAC) and environmental factors to establish policies, Hameed's method is decentralized, dynamic, and adaptable. The dynamic and flexible nature of access control is enhanced by Putra's approach, which integrates a Trust and Reputation approach to quantify node trust and reputation ratings. In restricted IoT environments, Siris [33] provides approaches that leverage smart contracts and interledger techniques for decentralized authorization, with an emphasis on tradeoffs between cost, latency, complexity, and privacy. The combined findings of these research demonstrate how blockchain technology may improve the effectiveness and security of IoT authorization systems.
- **Encryption:** Data is encrypted so that only authorized parties can decode it, protecting it both while it's in transit and at rest. IoT devices frequently use secure communication protocols like Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to encrypt data exchanged with servers or other devices. Data manipulation, eavesdropping, and illegal access to private information are all made more difficult by encryption.

  Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is suggested as an access control method for the IoT by Nakanishi [34] and Alsolami [35]. Specifically, Nakanishi [34] creates a distributed, fee-free, and scalable access control system by combining CP-ABE with IOTA technology. The throughput of access request processing can be greatly increased with this system's fine-grained attribute-based access control. Using CP-ABE to protect data from unwanted access, Alsolami [35] focuses on safeguarding smart homes. By putting out a modified CP-ABE technique with a constant size ciphertext that is appropriate for IoT devices with constrained memory and processing power, Yang [36] also contributes to this field. All of these research show that encryption, and especially CP-ABE, has great potential as an efficient access control method in the IoT.
- **Role-based Access Control (RBAC):** An organization or system's roles determine which devices or users are granted rights, and the RBAC access control paradigm is commonly used for this purpose. Permissions are linked to each role, and decisions about access are dependent on the

 doi:10.20944/preprints202405.0948.v1

roles that devices or users hold. Because RBAC centralizes rights and eliminates the need for unique user/device setups, it makes access management simpler.

Both Kumar [37] and Amoon [38] provide RBAC frameworks for IoT networks; Kumar concentrates on resource management and load balancing, while Amoon concentrates on thwarting malicious assaults. Abushmmala [39] builds on this work by using blockchain technology with RBAC to improve security and privacy in IoT applications for smart health.

- **Attribute-based Access Control:** ABAC expands access control beyond roles to take into account a variety of factors, including device properties, environmental factors, and user attributes. More precise control over access permissions is made possible by rules that assess these attributes as the basis for access decisions. In dynamic IoT systems, where access requirements may change depending on contextual factors, ABAC is especially helpful.

  ABAC integration is a promising method for improving security and controlling access, especially in the context of 5G networks [40]. This is further reinforced by the ABAC-CC framework proposal [41], which secures access and communication control to solve security and privacy concerns in Cloud-Enabled IoT (CE-IoT). Additionally, the application of ABAC in a cloud-enabled IoT environment is examined, emphasizing the use of the XACML language to build policy rules that block unwanted access to remote resources [42].
- **Network Segmentation:** Network segmentation is a technique used to isolate IoT devices and reduce the possible scope of security breaches. It entails splitting a network into distinct segments or subnetworks. Organizations may limit security risks and stop unwanted access to vital systems or data by isolating IoT devices into distinct network segments with controlled access.

  Novel approaches to network segmentation for IoT access control have been put forth in a number of research. In order to stop risks from spreading over the IoT networks, Lim [43] proposes a smart segmentation system that makes use of device features, network information, and service kinds. In order to minimize the attack surface, Vaere [44] presents Hopper, a security system that isolates each network host into a separate, access-controlled micro segment. A permission token segmentation approach based on blockchain is presented by Shi [45], which enables IoT access control systems to have fine-grained control over permissions. Wei [46] focuses on an SDN-based approach to fine-grained access control for IoT devices that efficiently
- **Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS):** To monitor and regulate network traffic, detect and prevent malicious activity or unauthorized access attempts, firewalls and IDS/IPS systems are used. These security precautions aid in preventing external threats or unauthorized users from compromising IoT devices to obtain private information or take control of the devices.

  In order to maintain the security of IoT networks and devices, IDS and IPS are essential. However, creating an efficient IDS for these networks is difficult because to the lightweight nature of IoT nodes [47]. In order to mitigate this issue, a resilient intrusion detection system architecture has been suggested, which reduces communication overhead and energy consumption while preserving elevated detection rates [48]. Furthermore, emphasis has been placed on the role Identity and Access Management (IAM) controls play in safeguarding IoT systems, with an emphasis on classifying and visualizing IAM technologies at the state of the art [49].

5. Related Study

Authentication and Access Control Mechanisms to Secure IoT Communications are popular and rapidly developing field of research. To assist researchers and developers in understanding what is going on in this field, many studies have been carried out, such as surveys, reviews, and SLR. This section covers the available and recent studies in the field along with a comparison table between these studies.

In [50], authors designed a comprehensive survey about scalable decentralized security framework for the future of IoT. Blockchain technology helps accomplish advantages like scalability and

 doi:10.20944/preprints202405.0948.v1

decentralization. Using message authentication and device verification will help in achieving network and device security levels. In order to provide device-to-device security, this framework takes advantage of the benefits of intelligent computing and tree-based hashing for device and request authentication. Requests are authenticated using a tree-based hash, and device-level security is provided via the framework's central authority-based security feature, which improves communication privacy and integrity. Delay, disconnection ratio, communication loss, and detection rate are the criteria analyzed in the experiment of the suggested security framework. A tree-based hash is used to maintain communication security while adhering to standard cryptographic procedures.

Fang et al. introduced [51] an overview of three different trust models analyzed in an IoT system design. It was suggested to use a flexible and effective strategy for secure data transmission and authentication that takes into account the many types of IoT devices. Through the efficient and effective use of IoT devices with greater processing power and storage, the suggested strategy offers security and privacy to resource-constrained IoT devices. Contextual privacy and data integrity services are also offered with secure data transmission. Using PUFs to protect T2 IoT devices against cloning attacks and streamline the authentication process based on one of the suggested trust models, a flexible and effective authentication and secure data transmission strategy is proposed. The suggested authentication strategy takes flexibility into account to apply various security measures to various kinds of IoT devices. ECC is used with hash algorithms and exclusive operations to meet efficiency requirements. The suggested approach accomplishes contextual privacy, forward security, end-to-end security, key escrow resilience, mutual authentication, initial session key agreement, data integrity, and anonymity. In order to verify the suggested scheme and security objectives, a security analysis is presented. Furthermore, an assessment of the scheme's performance is provided in relation to the other schemes concerning security features, computational cost, and communication overhead. The suggested approach offers flexible and efficient security by taking into account heterogeneous IoT devices, as demonstrated by the performance comparisons.

This study [52] proposed a novel method for building a large-scale blockchain-based IoT system. The users are provided with data storage optimization, security, privacy preservation, and a lightweight authentication mechanism by the suggested framework. This will guarantee that the suggested solution is a more safe, effective, and dependable authentication technique by utilizing the immutable and decentralized features of blockchain. The suggested approach can help with scalability and optimum storage, which is particularly helpful for the majority of applications that rely on blockchain technology. Hash evaluation and Message Authentication Code (MAC) verification are used in the suggested model. Furthermore, homomorphic encryption was incorporated to encrypt IoT data at the user's end and upload it to the cloud. Based on comprehensive simulation findings, the suggested method is contrasted with different benchmark frameworks. Because of its faster computation, connectedness, and mobility, the suggested framework transmission rate is higher than that of the current model. As a result, computing, communication, and packet delivery have all improved in terms of security and performance. The research's principal contribution is the creation of a revolutionary IoT strategy built on a trust-aware security approach, which improves security and privacy while connecting together exceptional IoT services.

The authors of this paper [53] indicated the concept of creating a more lightweight and safe authentication scheme, which was the main objective of creating this study. By using the Physically Unclonable Function (PUF) to offer physical security, the suggested protocol may store a single Challenge-Response Pair (CRP) for every sensor and doesn't require an extra phase for updating CRPs. The suggested protocol manipulates some fundamental cryptographic operations, such as bitwise-Exclusive-OR (XOR) and hash function, to achieve lightweight performance while simultaneously using three factors which are password, smartcard, and personal biometrics to strengthen security in comparison to two factors. Furthermore, the suggested protocol's security is shown by both informal and formal security analysis, which is based on Real-Or-Random (ROR). The suggested protocol is superior to the analogous protocols that are currently in use in terms of security, functionality, and

 doi:10.20944/preprints202405.0948.v1

computational costs. Lastly, an NS3 simulation assessing different network performance metrics shows that the suggested protocol works well in an IoT setting.

Alnefaie et al. [54] outlined the most important access control models along with their advantages and disadvantages, and their IoT extensions. The authors also looked into and examined the literature's current access control models and how well they worked for the IoT. A complete set of standards that should be significantly satisfied were defined to accomplish this purpose. The authors then reviewed the majority of access control methods and talked about their shortcomings in light of the specifications. With an emphasis on the architectural design of each solution, this survey collected traditional models and their extensions for IoT environments and their application scope. It then presented them clearly and accurately, before creating an IoT security mechanism, a set of requirements needed to be taken into account to better examine the reviewed access control model. The authors attempted to determine which access control model would work best for the IoT when paired with a suitable edge architecture. This combination must fulfill the specified IoT standards.

Faten et al. [55] proposed the application of RBAC, which grants rights and privileges based on entity roles. IoT devices have varying capacities for processing and managing data and they were made by various manufacturers using various technologies. Certain IoT devices had no computing power at all. This study builds a network of nodes, where each node is made up of various devices, some of which are limited and some of which are not. These devices will greatly improve each other's performance. The RBAC paradigm will be enforced by the blockchain to arrange the data flow between these nodes. To protect privacy, each node has a registration and authentication procedure that takes place before the data-sharing procedure. Two well-known Android apps for controlling IoT devices, one that makes use of the MQTT protocol and the other that makes use of Blockchain technology, are utilized to implement a realistic use case. When the data flow privacy of the two apps is compared, the IOTW app (an Android app that employs BC) performs significantly better.

This survey [56] presented a multi-agent system architecture that managed the delivery of decentralized and lightweight secure access control for the IoT using a private distributed blockchain. Building Blockchain Managers to secure IoT access control is the primary goal of the suggested approach. Furthermore, the system secures cloud computing, fog nodes, and IoT device connectivity as well as the overall IoT architecture. Because IoT devices have limited resources, the architecture uses a private hierarchical blockchain framework to fulfill their needs. Furthermore, the utilization of mobile agent software in our suggested solution demonstrates the high degree of mobility and intelligence of our solution and can significantly contribute to the decrease of traffic overheads. The authors created a scalable, general-purpose, and lightweight solution that can be used with a wide range of IoT applications.

A survey was presented in [57] to analyze the access control and authentication protocols of 19 well-known security cameras and connected doorbells. An exploit to obtain persistent access to IoT content was developed and tested. The findings showed that, after a password change or account cancellation, 16 out of 19 devices had an authentication or access control flaw that allowed an attacker to access an IoT device. A systematic flaw in access control and device authentication protocols for shared IoT ecosystems was found by the analysis. According to this research, vendors have a long way to go before they can fully integrate the security and privacy of content created by IoT devices.

In [58], a unique dynamic and secure access control (SDAC) concept was introduced for IoT networks. Through the use of wired and wireless networks (Cellular Networks or Wi-Fi), the suggested paradigm enables secure communication and information sharing between IoT devices. This paper primarily offered a fresh strategy by combining RBAC and ABAC. Additionally, by employing the concept of characteristics, the assignment of roles to users and permissions to roles are dynamic. The suggested SDAC model is more secure because it is built on RBAC model entities. Also, the characteristics of the objects and acts in this work make the permissions more stringent and complex. The generation of permissions, performance evaluations of the number of roles assigned, the duration of each permission assignment, and the memory usage of each entity are carried out. In comparison to

 doi:10.20944/preprints202405.0948.v1

earlier models that were offered, the performance of the proposed work was much improved. Unlike the conventional RBAC model, the SDAC is dynamic because it helps to reduce administrator burdens because all the processes including permission creation are done more efficiently.

In [59], a framework for trust-based access control was presented for decentralized IoT networks. In order to create a dynamic and reliable access control system, an extra TRS was created as part of a blockchain-based ABAC mechanism that takes trust and reputation ratings into account. Although the system is intended to operate on a public blockchain, private sidechains are used to store sensitive data including user attributes in order to protect user privacy. The framework was created to be blockchain agnostic, meaning it may be used with any blockchain platform that has sufficient support for the execution of smart contracts. A proof-of-concept was put into practice on a lab-scale testbed connected to a public Rinkeby Ethereum test network. The outcomes of the experiments show that the suggested structure can accomplish reliable processing latency and is workable for putting in place efficient access control in decentralized IoT networks.

Fotouhi M et al. [60] proposed a novel and safe authentication framework based on a lightweight hash chain for wireless body area networks used in healthcare IoT. Furthermore, the ROR model is used to conduct formal and informal security analysis. The ProVerif is used to validate the security verification of their framework. OPNET network is used to simulate their framework and compare it in terms of performance and security with other frameworks. The result shows that their framework is suitable for WBAN and more secure.

Behrad S et al. [61] proposed an effective mechanism called Slice Specific Authentication and Access Control (SSAAC). This mechanism utilizes virtualization technology's flexibility to improve the management of AAC on many devices. In this mechanism, the third-party providers inherit the authentication and access control privileges for IoT devices, reducing the communication load on the CN provider and enhancing 5G network flexibility and modularity. The Open Air Interface (OAI) is used to evaluate their mechanism's performance. Also, it includes the expected number of AAC signaling messages and the current status of AAC mechanisms in cellular networks in the evaluation process. Security requirements are highlighted in this proposal. As a result of this proposal, their mechanism proved its ability to overcome the security issues in the ACC of cellular networks. In addition, it minimizes the load of the ACC signaling on the CN communication providers.

Kumar P et al. [62] proposed a secure protocol called Secure Addressing and Mutual Authentication (SAMA). it is used to secure the network from different types of attacks or unauthorized access. SAMA is a novel authentication method to identify and authenticate a large number of devices in medical IoT networks. It takes into consideration three elements; the unique doctor's identity, the medical device, and the passwords. Furthermore, SAMA ensures confidentiality by using a unique session key to establish a secure connection between the server and the user. The performance evaluation process of SAMA depends on communication cost, computation, and functionality. In terms of security, the widely-accepted BAN logic model and AVISPA tool are used for formal and informal analysis. The results show that SAMA protects against multiple attacks like guessing the password, impersonation, and MITM.

Chaudhry S et al. [63] proposed an improved version of Das scheme [64] because it is unsafe against some types of attacks like MITM and impersonation attacks. This scheme aims to improve security, provide more secure communications, and increase computational efficiency. To achieve these goals, the iLACKA-IoT protocol is proposed. It protects against different types of attacks, especially MITM and impersonation attacks. A random or real (ROR) model is used to provide formal validation, and attack flexibility is discussed to provide informal validation. The results confirmed that the iLACKA-IoT protocol is better in terms of security and performance efficiency.

Panda et al. [65] proposed a mutual protocol based on ECC to protect IoT and its cloud services. AVISPA is used to verify the formal security of the proposed protocol. Then, it will be compared and informally analyzed with other protocols in the same field based on different security characteristics, like privacy, mutual authentication, reply, impersonation, and password attacks. Communication,

 doi:10.20944/preprints202405.0948.v1

computational storage overhead, and computational time are the factors that have been used in the performance evaluation. The results of the experiments proved that the proposed protocol is more secure and has better performance capabilities compared with other protocols.

Alladi et al. [66] proposed a lightweight authentication protocol named HARCI to achieve mutual authentication for medical IoT devices that suffer from limited memory, computational capabilities, and battery life. HARCI is designed with three layers for IoT architectures, which are patient nodes, sink nodes, and medical cloud servers. Unique session keys will be created for each phase of authentication in the two-stage authentication process. The secrecy and uniqueness of the session key will be ensured by using PUFs. PUFs are used for the dynamic generation of information needed in the authentication process. HARCI is safe against different types of attacks, like MITM, reply, and impersonation attacks. HARCI has multiple advantages, like data confidentiality, message integrity, protection for identity, and two-stage authentication. A formal evaluation of the security of the proposed protocol is performed to verify its validity. The proposed protocol is compared with other relevant protocols in terms of security and computation time to ensure its strength.

Trivedi H et al. [67] proposed a new authentication framework that includes TTP nomenclatured Secure Dynamic User Addition Protocol (SDUAP) which depends on JSON Web Token (JWT) utilizing private key cryptography. Their scheme contains 2 parts: Firstly, enhance scalability by authenticating the dynamic user addition protocol securely. It will help to allow new users to engage in current communication without affecting the entire system. Secondly, attribute-based encryption is used by non-identical entities to communicate continuously and securely in the dynamic distributed IoT. SDUAP security is evaluated using the Oracle model, and SDUAP resistance against different types of attacks is evaluated using the Scyther tool. Furthermore, SDUAP is compared with other relevant models in terms of storage, computation, and communication overhead.

Istiaque K et al. [68] presented a systematic literature review about machine learning for authentication and authorization in IoT. Recent developments in the field are discussed. Authentication and access control in IoT environments with focusing on machine learning are elaborated. Threats and challenges of authentication and authorization in IoT are analyzed. Different criteria to access a high level of security in IoT environments are determined. In the end, more discussion and analysis for future research direction to secure communications in IoT are provided.

Vishwakarma L et al. [69] proposed a new method known as SCAB-IoTA to provide a secure connection in IoT environments. Also, it confirms the authentication and authorization of IoT devices. In addition, SCAB-IoTA ensures data integrity. The proposed method used the blockchain with the integration of the Advanced Encryption Standard (AES) and the Elliptic Curve Digital Signature Algorithm. SCAB-IoTA aims to improve the security of IoT by preventing different attacks and reducing computational and storage overhead. Moreover, it uses Angular Distance (AD) to enable IoT device communication without any interruption. The results of the analysis ensure that SCAB-IoTA can resist different cyberattacks, like MITM and impersonation attacks.

Sivaselvan N et al. [70] proposed a novel and unified authentication and authorization system to secure IoT known as SUACC-IoT. SUACC-IoT depends on the capability concept which contains access privileges for authorized entities to access limited resources in the IoT networks. SUACC-IoT used the lightweight Elliptic Curve Diffie-Hellman Ephemeral cryptography technique, secret cryptography, hash function, and message authentication code. The analysis result proves that SUACC-IoT is secure against various types of attacks targeted IoT environments.

 doi:10.20944/preprints202405.0948.v1

Table 1. Existing work in this field.

Reference	Key Findings	Methodology	Limitations/Research Gaps
[50]	• A scalable decentralized security framework for the future of IoT. Blockchain technology helps accomplish advantages like scalability and decentralization. • Achieving network and device security levels by using message authentication and device verification. • Requests are authenticated using a tree-based hash. • A tree-based hash is used to maintain communication security while adhering to standard cryptographic procedures. • Device-level security is provided via the framework's central authority-based security feature.	• Blockchain to verify reliability. • A tree-based hash (which is used to maintain communication security while adhering to standard cryptographic procedures)	• Complexity of the system because of using decentralized security framework, intelligent computing, and Blockchain. • Suffering from performance problems when the networks expand. • Energy consumption and operational costs may be increased. • Needs to be updated continuously. • Privacy issues due to sharing sensitive information among users and devices in the blockchain.
[51]	• A flexible and effective strategy for secure data transmission and authentication was proposed. • The suggested strategy offers security and privacy to resource-constrained IoT devices. • Using PUFs to protect T2 IoT devices against cloning attacks and streamline the authentication process. • ECC is used with hash algorithms and XOR to meet efficiency requirements. • The suggested approach offers flexible and efficient security by taking into account heterogeneous IoT devices.	• Using PUFs which are one of the built-in security features of IoT devices. • Using ECC which is a lightweight asymmetric security solution to enhance secured transmission of data with hash algorithms and XOR.	• The study might not be able to cover every situation and security problem that IoT systems might encounter. • Assumptions made during the design and implementation of these trust models may restrict their effectiveness and create vulnerabilities in real-world IoT systems. • It can be difficult to guarantee security and compatibility across a variety of devices. • One potential drawback of the suggested authentication technique would be its scalability. • One drawback of the system would be how well it works in areas with limited resources, particularly when it comes to energy and computational overhead.

 doi:10.20944/preprints202405.0948.v1

Table 1. *Cont.*

Reference	Key Findings	Methodology	Limitations/Research Gaps
[52]	• A novel method for building a large-scale blockchain-based IoT system. • The users are provided with data storage optimization, security, privacy preservation, and a lightweight authentication mechanism. • Utilizing the immutable and decentralized features of blockchain. • Hash evaluation and MAC verification are used in the suggested model. • A homomorphic encryption was incorporated to encrypt IoT data at the user's end and upload it to the cloud.	• Blockchain • Hash evaluation and MAC verification • A homomorphic encryption (both symmetric and asymmetric encryption)	• There is just one way that was used to construct the suggested framework and it is built on a blockchain with permissions. Its flexibility and scalability might be restricted.
[53]	• Creating a more lightweight and safe authentication scheme. • By using a PUF to offer physical security, • The suggested protocol manipulates some fundamental cryptographic operations, such as bitwise-XOR and hash function, to achieve lightweight performance. • While simultaneously using three factors which are password, smartcard, and personal biometrics to strengthen security in comparison to two factors. • The suggested protocol is superior to the analogous protocols that are currently in use in terms of security, functionality, and computational costs.	• Using PUF. • Cryptographic operations, such as bitwise-XOR and hash function. • Using three factors which are password, smartcard, and personal biometrics.	• When the number of users and sensors in the IoT network rises dramatically, protocol performance may suffer. • It might not work with every kind of IoT device or communication protocol. • For certain IoT devices with limited resources, the protocol's resource needs could be too high.
[54]	• Outlined the most important access control models and how well they worked for the IoT. • Before creating an IoT security mechanism, a set of requirements needed to be taken into account in order to better examine the reviewed access control model. • The authors attempted to determine which access control model would work best for the IoT when paired with a suitable edge architecture. • This combination must fulfill the specified IoT standards.	• A SLR conducted about access control models for IoT.	• Designing access control models only for IoT in smart cities, smart homes, transportation, and healthcare fields. • Lack of detailed information for some solutions.

 doi:10.20944/preprints202405.0948.v1

Table 1. *Cont.*

Reference	Key Findings	Methodology	Limitations/Research Gaps
[55]	• The application of RBAC, which grants rights and privileges based on entity roles. • This study builds a network of nodes, where each node is made up of various devices, some of which are limited and some of which are not. • The RBAC paradigm will be enforced by the blockchain to arrange the data flow between these nodes. • To protect privacy, each node has a registration and authentication procedure that takes place before the data-sharing procedure. • Two well-known Android apps for controlling IoT devices, one that makes use of the MQTT protocol and the other that makes use of Blockchain technology, are utilized to implement a realistic use case.	• Using RBAC, which grants rights and privileges based on entity roles. • Blockchain • MQTT protocol for data transmission, as it is easy to implement and can communicate IoT data efficiently.	• One major problem is making sure blockchain-based systems can scale well to handle the growing amount of data created by IoT devices.
[56]	• A multi-agent system architecture that managed the delivery of decentralized and lightweight secure access control for the IoT using a private distributed blockchain. • Building Blockchain Managers to secure IoT access control is the primary goal of the suggested approach. • Because IoT devices have limited resources, the architecture uses a private hierarchical blockchain framework to fulfill their needs. • The utilization of mobile agent software in our suggested solution demonstrates the high degree of mobility and intelligence of our solution and can significantly contribute to the decrease of traffic overheads. • created a scalable, general-purpose, and lightweight solution that can be used with a wide range of IoT applications.	• Using a private hierarchical blockchain. • The utilization of mobile agent software to provide the high degree of mobility and intelligence.	• Performance problems could be among the limitations. After the suggested architecture is tested, these restrictions should become clearer.

 doi:10.20944/preprints202405.0948.v1

Table 1. *Cont.*

Reference	Key Findings	Methodology	Limitations/Research Gaps
[57]	• Analyze the access control and authentication protocols of 19 well-known security cameras and connected doorbells. • The findings showed that, after a password change or account cancellation, 16 out of 19 devices had an authentication or access control flaw that allowed an attacker to access an IoT device. • A systematic flaw in access control and device authentication protocols for shared IoT ecosystems was found by the analysis.	• All devices were connected to a WiFi network as part of the experiment setup, and two Android phones with companion applications were paired with each device. To simulate a shared IoT ecosystem, accounts were made on each phone to share access to the devices. After that, the researchers put the devices to the test to see how vulnerable they were to the suggested attack vector.	• A bigger sample size might offer a more thorough knowledge of the vulnerabilities in access control and authentication that are common in shared IoT environments. • The research concentrated on a particular kind of attack vector associated with unauthorized access and credential revocation.
[58]	• A unique dynamic and secure access control (SDAC) concept was introduced for IoT networks by using of wired and wireless networks. • Combining RBAC and ABAC. • By employing the concept of characteristics, the assignment of roles to users and permissions to roles are dynamic. • The suggested SDAC model is more secure because it is built on RBAC model entities. • The generation of permissions, performance evaluations of the number of roles assigned, the duration of each permission assignment, and the memory usage of each entity are carried out. • SDAC is dynamic because it helps to reduce administrator burdens because all the processes including permission creation are done more efficiently.	• Using a combination of RBAC and ABAC.	• The SDAC paradigm makes it easier to allocate roles based on permissions. The feature of conflicting roles and permissions is not covered by this paradigm. • In contrast to the conventional RBAC approach, the administrator must give more time to the object and action creation phase.

 doi:10.20944/preprints202405.0948.v1

Table 1. *Cont.*

Reference	Key Findings	Methodology	Limitations/Research Gaps
[59]	• A framework for trust-based access control was presented for decentralized IoT networks. • To create a dynamic and reliable access control system, an extra TRS was created as part of a blockchain-based ABAC mechanism that takes trust and reputation ratings into account. • Private blockchains are used to store sensitive data including user attributes to protect user privacy. • The outcomes of the experiments show that the suggested structure can achieve reliable processing latency and is workable for putting in place efficient access control in decentralized IoT networks.	• Private blockchains are used to store sensitive data and public blockchains. • using ABAC.	• Although attacks and access control violations are successfully captured by the Trust and Reputation System (TRS), violations in the attribute registration procedure within the sidechains may remain undetected.
[60]	• The ROR model is used to conduct formal and informal security analysis. • The ProVerif is used to validate the security verification of their framework. • OPNET network is used to simulate their framework and compare it in terms of performance and security with other frameworks. • The result shows that their framework is suitable for WBAN and more secure.	• Using a lightweight hash chain for authentication in wireless body area networks used in healthcare IoT	• They simulate each module individually because OPNET Network can't simulate cryptographic modules.

 doi:10.20944/preprints202405.0948.v1

Table 1. *Cont.*

Reference	Key Findings	Methodology	Limitations/Research Gaps
[61]	• An effective mechanism called Slice Specific Authentication and Access Control (SSAAC). • It utilizes virtualization technology's flexibility to improve the management of AAC on many devices. • The third-party providers inherit the authentication and access control privileges for IoT devices, reducing the communication load on the CN provider and enhancing 5G network flexibility and modularity. • OAI is used to evaluate their mechanism's performance. • Security requirements are highlighted in this proposal. • Their mechanism proved its ability to overcome the security issues in the ACC of cellular networks. In addition, it minimizes the load of the ACC signaling on the CN communication providers.	• Using virtualization technology's flexibility to improve the management of AAC on many devices.	• There is a need to apply various AAC mechanisms • OAI-CN needs to be modified by adding various network functions for third-party providers to implement different ACC mechanisms.
[62]	• A secure protocol called Secure Addressing and Mutual Authentication (SAMA) is proposed. • It is used to secure the network from different types of attacks or unauthorized access. • SAMA is a novel authentication method to identify and authenticate a large number of devices in medical IoT networks. • It takes into consideration three elements; the unique doctor's identity, the medical device, and the passwords. • The performance evaluation process of SAMA depends on communication cost, computation, and functionality. • In terms of security, the widely accepted BAN logic model and AVISPA tool are used for formal and informal analysis.	• SAMA ensures confidentiality by using a unique session key to establish a secure connection between the server and the user. • Using the hashing function for authentication.	• Not including dynamic identity authentication. • SAMA is not tested on real-world scenarios.

 doi:10.20944/preprints202405.0948.v1

Table 1. *Cont.*

Reference	Key Findings	Methodology	Limitations/Research Gaps
[63]	• An improved version of Das scheme [64] because it is unsafe against some types of attacks like MITM and impersonation attacks. • This scheme aims to improve security, provide more secure communications, and increase computational efficiency. • To achieve these goals, the iLACKA-IoT protocol is proposed. • The results confirmed that the iLACKA-IoT protocol is better in terms of security and performance efficiency.	• Using device access control. • A random or real (ROR) model is used to provide formal validation and attack flexibility is discussed to provide informal validation.	• Using specific software and hardware configurations in the evaluations, which may not include all IoT environments.
[65]	• A mutual protocol based on ECC to protect IoT and its cloud services. • Then, it will be compared and informally analyzed with other protocols in the same field based on different security characteristics, like privacy, mutual authentication, reply, impersonation, and password attacks. • Communication, computational storage overhead, and computational time are the factors that have been used in the performance evaluation. • The results of the experiments proved that the proposed protocol is more secure and has better performance capabilities compared with other protocols.	• Using ECC. • AVISPA is used to verify the formal security of the proposed protocol.	• There is a need for further enhancements to the computational time and overhead of the proposed protocol without affecting the security level. • The users need to know the reliability and behavior model of the proposed protocol before using it.

 doi:10.20944/preprints202405.0948.v1

Table 1. *Cont.*

Reference	Key Findings	Methodology	Limitations/Research Gaps
[66]	• HARCI is a lightweight authentication protocol to achieve mutual authentication for medical IoT devices that suffer from limited memory, computational capabilities, and battery life. • HARCI is designed with three layers for IoT architectures, which are patient nodes, sink nodes, and medical cloud servers. • PUFs are used for the dynamic generation of information needed in the authentication process. • HARCI is safe against different types of attacks, like MITM, reply, and impersonation attacks. • HARCI has multiple advantages, like data confidentiality, message integrity, protection for identity, and two-stage authentication.	• Unique session keys will be created for each phase of authentication in the two-stage authentication process. • The secrecy and uniqueness of the session key will be ensured by using PUFs.	• Lack of elaborate performance evaluation and limited details about scalability issues in real-world scenarios of medical IoT networks. • Lack of details about HARCI efficiency compared with other protocols in the same field.
[67]	• Their scheme contains 2 parts: Firstly, enhance scalability by authenticating the dynamic user addition protocol securely. It will help to allow new users to engage in current communication without affecting the entire system. • Secondly, attribute-based encryption is used by non-identical entities to communicate continuously and securely in the dynamic distributed IoT. • SDUAP is compared with other relevant models in terms of storage, computation, and communication overhead.	• A new authentication framework that includes TTP nomenclatured Secure Dynamic User Addition Protocol (SDUAP) which depends on JSON Web Token (JWT) utilizing private key cryptography. • SDUAP security is evaluated using the Oracle model, and SDUAP resistance against different types of attacks is evaluated using the Scyther tool.	• Lack of details about lightweight encryption and formal modes to enhance encryption techniques to prove the reliability and efficiency of their framework. • There is no focus on the privacy aspect of the SDUAP framework in the dynamic distributed IoT networks.

 doi:10.20944/preprints202405.0948.v1

Table 1. *Cont.*

Reference	Key Findings	Methodology	Limitations/Research Gaps
[68]	• A systematic literature review about machine learning for authentication and authorization in IoT. • Recent developments in the field are discussed. Authentication and access control in IoT environments with focusing on machine learning are elaborated. • Threats and challenges of authentication and authorization in IoT are analyzed. • Different criteria to access a high level of security in IoT environments are determined. • Detailed discussion and analysis for future research direction to secure communications in IoT are provided.	• Focusing on the ML approach.	• There is a need for detailed discussion about flexible, lightweight encryption techniques based on ML approaches.
[69]	• A new method known as SCAB-IoTA provides a secure connection in IoT environments. • It confirms the authentication and authorization of IoT devices. • SCAB-IoTA ensures data integrity. • SCAB-IoTA aims to improve the security of IoT by preventing different attacks and reducing computational and storage overhead. • It uses AD to enable IoT device communication without any interruption. • The results of the analysis ensure that SCAB-IoTA can resist different cyberattacks, like MITM and impersonation attacks.	• Using The proposed method used the blockchain with the integration of the AES and the Elliptic Curve Digital Signature Algorithm.	• The proposed method needs to be implemented in real-world environments, like IIoT, smart agriculture, and smart cities where different devices can reach each other securely and openly.
[70]	• A novel and unified authentication and authorization system to secure IoT known as SUACC-IoT. • SUACC-IoT depends on the capability concept which contains access privileges for authorized entities to access limited resources in the IoT networks. • The analysis result proves that SUACC-IoT is secure against various attacks targeted IoT environments.	• Using the lightweight Elliptic Curve Diffie-Hellman Ephemeral cryptography technique, secret cryptography, hash function, and message authentication code.	• Need for a decentralized environment to make their system more scalable. • Mobility management issues in IoT networks need to be considered. • Bilateral access control and fine-granularity need to be Integrated to protect the privacy in the proposed protocol.

 doi:10.20944/preprints202405.0948.v1

6. Challenges and Future Directions

The challenges of IoT security authentication and access control will be discussed in this section. Furthermore, we'll talk about the future directions to solve these issues, which could lead to an IoT ecosystem that is safer and more reliable.

6.1. Challenges in IoT security

IoT security suffers from different challenges regarding authentication and access control. In this section, we will present these challenges as follows:

1. Variations in device design and challenges in putting standard mechanisms into practice [71].
2. To improve authentication and authorization, a decentralized IoT access control architecture that makes use of OAuth and decentralized identity technology is required [72].
3. Strong access control systems are required, especially given the explosive expansion of the IoT and the production of sensitive data [73].
4. To address security and privacy problems in the IoT, lightweight and interoperable authentication protocols are required [74].
5. The requirement for more reliable authorization and authentication mechanisms makes the application of machine learning techniques essential. According to [68].
6. It is necessary to investigate how hybrid deep learning techniques, namely the fusion of physiological and behavioral characteristics, might improve Internet of Things security [75].

6.2. Future Directions

In this section, we will focus on future research directions for IoT security which are presented as follows:

1. Investigating the possibilities for improving IoT security offered by revolutionary technologies like blockchain, artificial intelligence, and 5G networks, as well as solving the open issues in creating comprehensive, lightweight, and scalable security frameworks for the IoT.
2. Offering effective and safe IoT authentication techniques with the goal of improving the security of IoT environments. In addition to potentially looking into new methods or technologies to address the security issues in IoT systems, this could entail further research and development of authentication protocols based on encryption cryptography.
3. concentrating on approaches for authorization and authentication that have a high level of security, good throughput, low computational cost, and good tolerance.
4. Investigating the creation of ML-driven authorization systems to improve the security of IoT environments, taking into account a hybrid strategy that combines centralized and distributed techniques to successfully solve security concerns.
5. Developing lightweight platforms for blockchain implementation, investigating novel consensus algorithms appropriate for IoT devices, optimizing blockchain technology for resource-constrained IoT environments, and improving blockchain's security and privacy features for IoT applications. Scalability and effectiveness of blockchain technology in IoT can be the subject of future research.
6. In order to apply blockchain-based access control approaches, it is necessary to analyze the interaction between authentication and authorization techniques and research paradigms like fog computing, multi-access edge computing, and dew computing.

7. Conclusions

This paper concludes by offering a comprehensive review of access control and authentication strategies to secure IoT communications. The paper emphasizes the significance of strong security measures in IoT environments by looking at a variety of authentication methods, including certificate-based, biometric, and multi-factor authentication, as well as access control mechanisms, including attribute-based and role-based access control. In order to reduce security threats, the study examines

 doi:10.20944/preprints202405.0948.v1

and provides insights into IoT security challenges. In general, the study offers significant suggestions to practitioners, researchers, and policymakers for improving the security of Internet of Things systems.

Author Contributions: All authors equally contributed. All authors have read and agreed to the published version of the manuscript.

Funding: This paper was funded by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia under the [GRANT].

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors extend their appreciation to the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [GRANT]. The authors would like to thank the anonymous reviewers for their insightful scholastic comments and suggestions, which improved the quality and clarity of the paper.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
ECC	Elliptic Curve Cryptography
OTP	One-Time Password
SRPP	Secure Remote Password Protocol
PKI	Public Key Infrastructure
DNS	Domain Name System
DANE	DNS-based Authentication of Named Entities protocol
DNSSEC	DNS's Security Extensions
CA	Certificate Authority
MITM	Man-In-The-Middle attack
MFA	Multi-Factor Authentication
DIES	Data Inverting Encoding Scheme
ABAC	Attribute-Based Access Control
TLS	Transport Layer Security
SSL	Secure Sockets Layer
RBAC	Role-based Access Control
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
IAM	Identity and Access Management
MAC	Message Authentication Code
PUF	Physically Unclonable Function
CRP	Challenge-Response Pair
XOR	bitwise-Exclusive-OR
ROR	Real-Or-Random
OAI	Open Air Interface
AES	Advanced Encryption Standard
AD	Angular Distance

References

1. Michailidis, E.T.; Vouyioukas, D. A review on software-based and hardware-based authentication mechanisms for the Internet of Drones. *Drones* **2022**, *6*, 41.
2. Mehta, M.; Baldaniya, H.; Goriya, N. A Systematic Review of Authentication Methods for Internet of Things. In Proceedings of the 2020 IEEE International Conference for Innovation in Technology (INOCON). IEEE, 2020, pp. 1–6.

 doi:10.20944/preprints202405.0948.v1

3. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Trust management in decentralized iot access control system. In Proceedings of the 2020 IEEE international conference on blockchain and cryptocurrency (ICBC). IEEE, 2020, pp. 1–9.
4. Hammi, B.; Fayad, A.; Khatoun, R.; Zeadally, S.; Begriche, Y. A lightweight ECC-based authentication scheme for Internet of Things (IoT). *IEEE Systems Journal* **2020**, *14*, 3440–3450.
5. Alshahrani, F.S.; Abdullah, M. Graphical-based password for user authentication in internet of things. *Indonesian Journal of Electrical Engineering and Computer Science* **2022**, *28*, 1139–1146.
6. Tarish, H.A. Enhanced IoT Wi-Fi protocol standard's security using secure remote password. *Periodicals of Engineering and Natural Sciences* **2022**, *10*, 632–644.
7. Höglund, J.; Lindemer, S.; Furuhed, M.; Raza, S. PKI4IoT: Towards public key infrastructure for the Internet of Things. *Computers & Security* **2020**, *89*, 101658.
8. Belattaf, S.; Mohammedi, M.; Omar, M.; Aoudjit, R. Reliable and adaptive distributed public-key management infrastructure for the Internet of things. *Wireless Personal Communications* **2021**, *120*, 113–137.
9. Joseph Antony, A.; Singh, K. A Blockchain-Based Public Key Infrastructure For IoT-Based Healthcare Systems. *The Computer Journal* **2024**, *67*, 1531–1537.
10. Balakrichenan, S.; Ayoub, I.; Ampeau, B. PKI for IoT using the DNS infrastructure. In Proceedings of the 2022 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA). IEEE, 2022, pp. 1–8.
11. Karthikeyan, S.; Poongodi, T. Secured Data Compression and Data Authentication in Internet of Thing Networks Using LZW Compression Based X. 509 Certification. In Proceedings of the 2022 IEEE International Conference on Data Science and Information System (ICDSIS). IEEE, 2022, pp. 1–5.
12. Garba, A.; Khoury, D.; Balian, P.; Haddad, S.; Sayah, J.; Chen, Z.; Guan, Z.; Hamdan, H.; Charafeddine, J.; Al-Mutib, K. LightCERT4IoTs: Blockchain-based lightweight certificates authentication for IoT applications. *IEEE Access* **2023**, *11*, 28370–28383.
13. Malik, M.; Dutta, M.; Granjal, J.; et al. L-ecqv: Lightweight ecqv implicit certificates for authentication in the internet of things. *IEEE Access* **2023**, *11*, 35517–35540.
14. Seitz, L.; Selander, G.; Wahlstroem, E.; Erdtman, S.; Tschofenig, H. Authentication and Authorization for Constrained Environments Using the OAuth 2.0 Framework (ACE-OAuth). *RFC* **2022**, *9200*, 1–72.
15. Chen, J.; Hoppen, M.; Böken, D.; Reitz, J.; Schluse, M.; Roßmann, J. Identity, authentication and authorization in forestry 4.0 using oauth 2.0. In Proceedings of the 2022 3rd International Informatics and Software Engineering Conference (IISEC). IEEE, 2022, pp. 1–6.
16. Oh, S.R.; Koo, J.; Kim, Y.G. Security interoperability in heterogeneous IoT platforms: threat model of the interoperable OAuth 2.0 framework. In Proceedings of the Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing, 2022, pp. 22–31.
17. Ahmed, N.A.; Ammar, M.; Hefny, H.A. Proposed authentication protocol for IoT using blockchain and fog nodes. *International Journal of Advanced Computer Science and Applications* **2020**, *11*.
18. Hameed, K.; Garg, S.; Amin, M.B.; Kang, B. A formally verified blockchain-based decentralised authentication scheme for the internet of things. *The Journal of Supercomputing* **2021**, *77*, 14461–14501.
19. Manogaran, G.; Rawal, B.S.; Saravanan, V.; MK, P.; Xin, Q.; Shakeel, P. Token-based authorization and authentication for secure internet of vehicles communication. *ACM Transactions on Internet Technology* **2023**, *22*, 1–20.
20. Sonth, R.R.; Pranamya, Y.; Harish Kumar, N.; Deepak, G. A Survey on Methodologies and Algorithms for Mutual Authentication in IoT Devices. In Proceedings of the Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020. Springer, 2021, pp. 309–315.
21. Mbarek, B.; Ge, M.; Pitner, T. An efficient mutual authentication scheme for internet of things. *Internet of things* **2020**, *9*, 100160.
22. Jiang, L.; Cui, H. Private and Mutual Authentication Protocols for Internet of Things. *Mathematics* **2023**, *11*, 1929.
23. Golec, M.; Gill, S.S.; Bahsoon, R.; Rana, O. BioSec: A biometric authentication framework for secure and private communication among edge devices in IoT and industry 4.0. *IEEE Consumer Electronics Magazine* **2020**, *11*, 51–56.
24. Bedari, A.; Wang, S.; Yang, W. A secure online fingerprint authentication system for industrial IoT devices over 5G networks. *Sensors* **2022**, *22*, 7609.

 doi:10.20944/preprints202405.0948.v1

25. Kameswara Rao, M.; Santhi, S. A novel user authentication protocol using biometric data for iot networks. In Proceedings of the Rising Threats in Expert Applications and Solutions: Proceedings of FICR-TEAS 2020. Springer, 2021, pp. 85–91.
26. Alsellami, B.M.; Deshmukh, P.D. The recent trends in biometric traits authentication based on internet of things (IoT). In Proceedings of the 2021 international conference on artificial intelligence and smart systems (ICAIS). IEEE, 2021, pp. 1359–1365.
27. Mishra, A.K.; Wazid, M. Design of a cloud-based security mechanism for Industry 4.0 communication. In Proceedings of the 2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC). IEEE, 2023, pp. 337–343.
28. Saqib, M.; Jasra, B.; Moon, A.H. A lightweight three factor authentication framework for IoT based critical applications. *Journal of King Saud University-Computer and Information Sciences* **2022**, *34*, 6925–6937.
29. Mohammad, A.; Al-Refai, H.; Alawneh, A.A. User authentication and authorization framework in IoT protocols. *Computers* **2022**, *11*, 147.
30. Sudha, M.; Rajendiran, M.; Specht, M.; Reddy, K.S.; Sugumaran, S. A low-area design of two-factor authentication using DIES and SBI for IoT security. *The Journal of Supercomputing* **2022**, *78*, 4503–4525.
31. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R.; Ignjatovic, A. Trust-based blockchain authorization for iot. *IEEE Transactions on Network and Service Management* **2021**, *18*, 1646–1658.
32. Hameed, K.; Raza, A.; Garg, S.; Amin, M.B. A Blockchain-based Decentralised and Dynamic Authorisation Scheme for the Internet of Things. *arXiv preprint arXiv:2208.07060* **2022**.
33. Siris, V.A.; Dimopoulos, D.; Fotiou, N.; Voulgaris, S.; Polyzos, G.C. Decentralized authorization in constrained IoT environments exploiting interledger mechanisms. *Computer Communications* **2020**, *152*, 243–251.
34. Zhang, Y.; Nakanishi, R.; Sasabe, M.; Kasahara, S. Combining IOTA and attribute-based encryption for access control in the Internet of Things. *Sensors* **2021**, *21*, 5053.
35. Alsolami, H.; Bamasag, O.; Aljahdali, A. A Novel Access Control Security Model Based on Ciphertext Policy Attribute-Based Encryption for Smart Homes. In Proceedings of the Proceedings of the 4th International Conference on Future Networks and Distributed Systems, 2020, pp. 1–5.
36. Yang, W.; Wang, R.; Guan, Z.; Wu, L.; Du, X.; Guizani, M. A lightweight attribute based encryption scheme with constant size ciphertext for internet of things. In Proceedings of the ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020, pp. 1–6.
37. Kumar, R.; Agrawal, N. RBAC-LBRM: An RBAC-based load balancing assisted efficient resource management framework for IoT-edge-fog network. *IEEE Sensors Letters* **2022**, *6*, 1–4.
38. Amoon, M.; Altameem, T.; Altameem, A. RRAC: Role based reputed access control method for mitigating malicious impact in intelligent IoT platforms. *Computer Communications* **2020**, *151*, 238–246.
39. Abushmmala, F.F.; AbuSamra, A.A. Blockchain-Based Secure Smart Health IoT solution Using RBAC Architecture. *Journal of Engineering Research and Technology* **2023**, *10*.
40. Kaven, S.; Skwarek, V. Poster: Attribute based access control for IoT devices in 5G networks. In Proceedings of the Proceedings of the 28th ACM Symposium on Access Control Models and Technologies, 2023, pp. 51–53.
41. Bhatt, S.; Sandhu, R. Abac-cc: Attribute-based access control and communication control for internet of things. In Proceedings of the Proceedings of the 25th ACM Symposium on Access Control Models and Technologies, 2020, pp. 203–212.
42. Sifou, F.; AlShahwan, F.; Hammoud, A.; Marwan, M.; Hammouch, A. Implementing Policy Rules in Attributes Based Access Control with XACML within Cloud-Enabled IoT Environment. *J. Commun.* **2020**, *15*, 107–112.
43. Lim, J.; Sohn, S.; Kim, J. Proposal of Smart Segmentation Framework for preventing threats from spreading in IoT. In Proceedings of the 2020 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2020, pp. 1745–1747.
44. De Vaere, P.; Tulimiero, A.; Perrig, A. Hopper: Per-Device Nano Segmentation for the Industrial IoT. In Proceedings of the Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, 2022, pp. 279–293.
45. Shi, J.; Li, R. Permission Token Segmentation Scheme Based on Blockchain Access Control. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2020, pp. 1956–1964.

 doi:10.20944/preprints202405.0948.v1

46. Wei, M.; Liang, E.; Nie, Z. A SDN-based IoT fine-grained access control method. In Proceedings of the 2020 International Conference on Information Networking (ICOIN). IEEE, 2020, pp. 637–642.
47. Anitha, A.A.; Arockiam, L. A review on intrusion detection systems to secure IoT networks. *International Journal of Computer Networks and Applications* **2022**, *9*, 38–50.
48. Al Qurashi, M.; Angelopoulos, C.M.; Katos, V. An architecture for resilient intrusion detection in IoT networks. In Proceedings of the ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020, pp. 1–7.
49. Ward, G.; Janczewski, L. Analysis of Identity Access Management Controls in IoT Systems. In Proceedings of the 2022 IEEE 7th International conference for Convergence in Technology (I2CT). IEEE, 2022, pp. 1–7.
50. Sheron, P.F.; Sridhar, K.; Baskar, S.; Shakeel, P.M. A decentralized scalable security framework for end-to-end authentication of future IoT communication. *Transactions on Emerging Telecommunications Technologies* **2020**, *31*, e3815.
51. Fang, D.; Qian, Y.; Hu, R.Q. A flexible and efficient authentication and secure data transmission scheme for IoT applications. *IEEE Internet of Things Journal* **2020**, *7*, 3474–3484.
52. Al Hwaitat, A.K.; Almaiah, M.A.; Ali, A.; Al-Otaibi, S.; Shishakly, R.; Lutfi, A.; Alrawad, M. A new blockchain-based authentication framework for secure IoT networks. *Electronics* **2023**, *12*, 3618.
53. Liu, Z.; Guo, C.; Wang, B. A physically secure, lightweight three-factor and anonymous user authentication protocol for IoT. *IEEE Access* **2020**, *8*, 195914–195928.
54. Alnefaie, S.; Alshehri, S.; Cherif, A. A survey on access control in IoT: Models, architectures and research opportunities. *International Journal of Security and Networks* **2021**, *16*, 60–76.
55. Abushmmala, F.F.; AbuSamra, A.A. Blockchain-Based Secure Smart Health IoT solution Using RBAC Architecture. *Journal of Engineering Research and Technology* **2023**, *10*.
56. Algarni, S.; Eassa, F.; Almarhabi, K.; Almalaise, A.; Albassam, E.; Alsubhi, K.; Yamin, M. Blockchain-based secured access control in an IoT system. *Applied Sciences* **2021**, *11*, 1772.
57. Janes, B.; Crawford, H.; OConnor, T. Never ending story: Authentication and access control design flaws in shared iot devices. In 2020 IEEE Security and Privacy Workshops (SPW), 2020.
58. Aftab, M.U.; Oluwasanmi, A.; Alharbi, A.; Sohaib, O.; Nie, X.; Qin, Z.; Ngo, S.T. Secure and dynamic access control for the Internet of Things (IoT) based traffic system. *PeerJ Computer Science* **2021**, *7*, e471.
59. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R.; Ignjatovic, A. Trust-based blockchain authorization for iot. *IEEE Transactions on Network and Service Management* **2021**, *18*, 1646–1658.
60. Fotouhi, M.; Bayat, M.; Das, A.K.; Far, H.A.N.; Pournaghi, S.M.; Doostari, M.A. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Computer Networks* **2020**, *177*, 107333.
61. Behrad, S.; Bertin, E.; Tuffin, S.; Crespi, N. A new scalable authentication and access control mechanism for 5G-based IoT. *Future Generation Computer Systems* **2020**, *108*, 46–61.
62. Kumar, P.; Chouhan, L. A privacy and session key based authentication scheme for medical IoT networks. *Computer Communications* **2021**, *166*, 154–164.
63. Chaudhry, S.A.; Yahya, K.; Al-Turjman, F.; Yang, M.H. A secure and reliable device access control scheme for IoT based sensor cloud systems. *Ieee Access* **2020**, *8*, 139244–139254.
64. Das, A.K.; Wazid, M.; Yannam, A.R.; Rodrigues, J.J.; Park, Y. Provably secure ECC-based device access control and key agreement protocol for IoT environment. *IEEE Access* **2019**, *7*, 55382–55397.
65. Panda, P.K.; Chattopadhyay, S. A secure mutual authentication protocol for IoT environment. *Journal of Reliable Intelligent Environments* **2020**, *6*, 79–94.
66. Alladi, T.; Chamola, V.; et al. HARCI: A two-way authentication protocol for three entity healthcare IoT networks. *IEEE Journal on Selected Areas in Communications* **2020**, *39*, 361–369.
67. Trivedi, H.S.; Patel, S.J. Design of secure authentication protocol for dynamic user addition in distributed Internet-of-Things. *Computer Networks* **2020**, *178*, 107335.
68. Istiaque Ahmed, K.; Tahir, M.; Hadi Habaebi, M.; Lun Lau, S.; Ahad, A. Machine learning for authentication and authorization in iot: Taxonomy, challenges and future research direction. *Sensors* **2021**, *21*, 5122.
69. Vishwakarma, L.; Das, D. SCAB - IoTA: Secure communication and authentication for IoT applications using blockchain. *Journal of Parallel and Distributed Computing* **2021**, *154*, 94–105. https://doi.org/https://doi.org/10.1016/j.jpdc.2021.04.003.

 doi:10.20944/preprints202405.0948.v1

70. Sivaselvan, N.; Bhat, K.V.; Rajarajan, M.; Das, A.K.; Rodrigues, J.J. SUACC-IoT: Secure unified authentication and access control system based on capability for IoT. *Cluster Computing* **2023**, *26*, 2409–2428.
71. Tinnaluri, V.N.; Babu, A.J.; Shanmugaraja, P.; Kumar, S.S.; AdityPai, H. A Productive Model for Secured Data Sharing in Blockchain Technology based IoT. In Proceedings of the 2023 International Conference on Inventive Computation Technologies (ICICT). IEEE, 2023, pp. 1426–1431.
72. Kang, J.H.; Seo, M. Enhanced Authentication for Decentralized IoT Access Control Architecture. *Cryptography* **2023**, *7*, 42.
73. Mishra, R.; Yadav, R. Access control in IoT networks: analysis and open challenges. In Proceedings of the Proceedings of the International Conference on Innovative Computing & Communications (ICICC), 2020.
74. Sahoo, A.; Sahoo, S.S.; Sahoo, S.; Sahoo, B.; Turuk, A.K. An interoperable ECC based authentication and key agreement scheme for IoT environment. In Proceedings of the 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS). IEEE, 2020, pp. 419–426.
75. Chen, J.I.Z.; Lai, K.L. Internet of Things (IoT) authentication and access control by hybrid deep learning method-a study. *Journal of Soft Computing Paradigm (JSCP)* **2020**, *2*, 236–245.