Article available at Al-Baha University Journal of Basic and Applied Sciences

Journal of Basic and Applied Sciences

Journal homepage: https://portal.bu.edu.sa/web/jbas/

A Novel Methodology for Blockchain Technology-Based Access Control Model for Preserving Privacy in the IoT's

Mohammed Al Qurashi*

Faculty of Computer Science & Information Technology, Al-Baha University, Al-Aqiq, Saudi Arabia

ARTICLE INFO

Article history:
Received 13 Feb., 2023
Received in revised form
14 April, 2023
Accepted 1 June, 2023

Keywords:
Access Control
Internet of Things
Blockchain
Security
Privacy

ABSTRACT

Access control in IoT refers to controlling who has access to certain devices or networks within the Internet of Things. This is important for ensuring the security and privacy of the data and systems within the IoT. Access control can be implemented through user authentication, permission-based access, encryption, and network segmentation. It is essential to consider IoT access control measures carefully to ensure data and systems security and privacy. Access control measures must be tailored to the particular environment, device, and data within the IoT to provide adequate protection. Furthermore, access control measures must be regularly monitored and tested to ensure that they remain effective and up-to-date. Regular monitoring and testing of access control measures in the IoT is essential, as threats and vulnerabilities are constantly evolving. As such, the implementation of effective access control measures in the IoT can provide a significant layer of security and privacy for data and systems. Given the significance of security and privacy in IoT devices, we propose a methodology that addresses all aspects of security and privacy in this study. This study aims to propose a methodology that addresses all aspects of security and privacy in IoT devices, specifically related to access control measures. This study will provide important guidelines for researchers and security solution providers working on IoTs, such as identifying, designing, testing, and deploying an access control system, particularly with the help of blockchain technology. The proposed methodology consists of seven phases. The contribution of this study is to provide a significant layer of security and privacy for data and systems within the IoT by implementing effective access control measures. By implementing this methodology, we hope to achieve secure and efficient access control solutions for a wide range of IoT applications.

1. Introduction

The Internet of Things (IoT) is a ubiquitous concept in which diverse items in the environment communicate and collaborate through wired and wireless connections to share services and accomplish shared objectives [1]. Making the world smart enough to enable the emergence of more intelligent transportation, energy, healthcare, and other spheres of life is the goal of the IoT [2]. The IoT's primary goal is connecting objects with any other objects at any time and place.

To achieve this, IoT technology provides end-to-end digital communication between physical devices, empowering them with the ability to sense and interact with their surroundings [3]. The ability of IoT devices to interact with their environment is a critical aspect of the technology, providing for the creation of "smart cities," in which objects have a wide range of applications, including energy efficiency, public safety, improved healthcare, and more [5].

By linking physical and virtual items, the IoT's global network architecture allows for data transmission features such as autonomous data collection, event transfer, network connection, and interoperability [5]. IoT device accessibility and connection have expanded, making them more vulnerable to security risks such as spoofing, tempering, repudiation, confidentiality, and user privacy [6]. Users' privacy options include query privacy and location privacy. The mining of private data is related to privacy queries. Location privacy is safeguarding a user's sensitive information, including their home address, behavior, health state, and other sensitive information [7]. It is concerning that IoT devices are easily accessible and provide a means for users' private data to be accessed and mined without their knowledge or consent. With the introduction of IoT devices, protecting a user's privacy is more important than ever.

IoT devices include a GPS system built-in for placing location data. If the user wants to know where they are, they may ask for location-based services (LBS) [8]. The search might be for the

* Corresponding author Dr. Mohammed Al Qurashi: .

E-mail address: malqurashi@bu.edu.sa.
1658-7537/© 20223 BUJBAS. Published by Al-Baha University. All rights reserved.

closest restaurant, hospital, park, or other exciting spots. The user's location and identity are included in the inquiry. Utilising LBS services is convenient, however, there are privacy risk problems that arise. An adversary might simply connect the user's identity and location based on the information supplied in order to get further private information. When obtaining and disseminating information, security and privacy are crucial factors to take into account. This data and information must be protected against unauthorized and unlawful access. The IoT gadgets we use in our homes, businesses, streets, and buildings continually transfer information to one another and to the Internet [9]. Sensitive information about an individual is included in the data shared. This data may be exposed, which would pose a major privacy risk. However, it's crucial to preserve device users' privacy by not disclosing their location. Three general approaches may be used to secure location privacy [10]. The first technique uses location anonymisation based on temporal and spatial clocking to protect the user's actual position. The second idea under consideration is location obfuscation, a method for protecting user privacy that involves slightly blurring or introducing noise to the user's real position. The third approach is focused on private information retrieval (PIR), which is currently difficult to use in practical situations.

New technologies such as blockchain and strong encryption could be used to help protect user data, ensuring that a user's private information is not accessed without their consent. These new technologies, while still in their infancy, have the potential to provide a secure and reliable means of protecting a user's privacy. However, a lot of work still needs to be done to ensure that these new technologies effectively protect users' privacy.
The paper is organized as follows: Section 2 discusses the importance of access control. Section 3 details the role of blockchain in maintaining privacy in the Internet of Things. Section 4 provides related work and identifies research gaps. In section 5, the methodology is proposed. Finally, section 6 concludes the work.

2. Importance of Access Control

Access control is the selective restriction of access to a place or other resource. The purpose of access control is security, whether it is physical security, computer security, or information security [11]. Access control systems can be used to restrict entrance to a building or specific areas within a building and grant access to authorized individuals [12]. There are several types of access control systems, each with its own advantages and disadvantages. The most common type of access control system is the electronic key card system. This system uses cards with encoded magnetic strips or chips that must be presented in order to gain entry. The advantage of this system is that it is relatively cheap and easy to maintain. The disadvantage is that unauthorised individuals can use lost or stolen cards to gain entry. Another type of access control system is the biometric system. This system uses physical characteristics such as fingerprints, handprints, or iris scans to identify authorised individuals [14]. The advantage of this system is that it is very difficult for unauthorised individuals to gain access; however, the disadvantage is that it can be expensive to implement and maintain. The final type of access control system is the token-based system. This system requires users to possess a physical token, such as a key or badge, in order to gain entry. The advantage of this system is that it provides good security; however, the disadvantage is that unauthorised individuals can use lost or stolen tokens to gain entry.

There are three main types of access control systems: physical, logical, and administrative.

1. Physical access control systems restrict physical access to a facility or equipment. Physical access can be controlled through the use of security devices such as locks, keys, biometrics, and security guards.

2. Logical access control systems restrict logical access to computer systems and information. Logical access can be controlled through the use of passwords, user IDs, firewalls, and encryption.

3. Administrative access control systems restrict administrative access to facilities, equipment, and information. Administrative access can be controlled through the use of policies and procedures, job descriptions, security clearances, and security training.

Access Control in IOT is a security measure that allows organizations to control the flow of data and prevent unauthorized access to their IoT devices. It allows an organization to limit who has access to its connected devices while also providing visibility into who is accessing the device, when they are accessing it, and what they are doing with it [14]. Implementing an effective access control policy can help mitigate risks associated with malicious external actors or rogue internal users accessing private data or modifying system settings and help maintain compliance with data privacy regulations such as The Global Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) [15]. An effective access control policy for IoT devices is an essential security measure that should not be overlooked.

2.1. How to choose the right access control system

Access control is a security technique that can be used to regulate who or what can view or use resources in a computing environment. Having an access control system in place is important as it can help prevent unauthorised access and data breaches [16]. There are different types of access control systems, and the one that is right for your business will depend on your specific needs and requirements. When choosing an access control system, there are a few things you should keep in mind.

2.2. The type of business you have

The access control system you choose should be appropriate for your size and business. A simple password-protection system might suffice if the business is of a small size. However, a larger business with sensitive data will need a more robust system [17].

2.3. Budget for access control

Access control systems can vary greatly in price, so setting a budget before beginning your search is important. In contrast, the most expensive option is not necessarily the best for business [18].

2.4. Security requirements

Assess the security needs before choosing an access control system. What kind of data do you need to protect? How many users will need access to the system? What level of security do you require? Once you know the answers to these questions, you can narrow down your choices and select the best system for your business [19].

3. Role of Blockchain in Maintaining Privacy in the Internet of Things

We live in an age where data is becoming increasingly valuable. As technology advances and the number of connected devices increases, the amount of data being generated is growing exponentially. With this growth, however, comes an ever-increasing threat to our privacy. Data security and privacy protection have become major concerns in recent years, particularly with the emergence of the IoT. Fortunately, blockchain technology has emerged as a viable solution for making sure our data remains secure.

In the IoT, blockchain can play a role in maintaining privacy in a number of ways. For example, blockchain can be used to decentralize data storage, which would make it more difficult for hackers to access sensitive data [20]. Additionally, blockchain can be used to create tamper-proof records of data, which would help to ensure that data is not altered or deleted without authorization. Finally, blockchain can be used for anonymous communication between devices, which would help to prevent eavesdropping and other forms of surveillance. Blockchain has the potential to play a major role in ensuring privacy in the IoT. By creating a decentralized ledger of data, blockchain can help to provide transparency and accountability in the way data is collected and used. [21] Additionally, blockchain can help ensure that data is only accessed by those authorized to do so. This could potentially prevent data breaches and protect the privacy of individuals and businesses alike. By creating a decentralized and encrypted ledger, blockchain can provide high security and privacy for data transfers. In addition, blockchain can help to ensure the authenticity of data, as each block in the chain contains a timestamp and signature that can be verified [22]. Blockchain technology can thus help to create a more secure and private IoT, where data is protected from tampering or theft. This could have wide-ranging implications for industries such as healthcare, finance, and smart cities, which are all increasingly relying on interconnected devices [23].

4. Related Work

A new framework for IoT access control is proposed by [24] and is based on blockchain technology. Authors in the study [25] provide a novel approach to access management in the IoT based on the emerging "Block Chain" technology, which aids users in accessing or managing their data. Machine learning and deep learning algorithms must be used to handle the massive amounts of raw data generated by sensors. This will enable the creation of an intelligent knowledge base that will enable the provision of the necessary solutions as and when they are needed [26]. The study addresses the drawbacks of the centralized approach to IoT security and suggests the blockchain method as a successful distributed solution to provide security and privacy to IoT devices in the future. In order to ensure precise access control functions for IoT devices with a strong guarantee of anonymity for IoT end users, FairAccess and PPDAC, a lightweight and privacy-preserving access control framework built on emerging blockchain technology, primarily the permissionless and public type, is introduced in this direction [27]. Authors [28] examine the security and privacy concerns in the 5G-VANET with SDN enabled in the transportation system and the vehicular IoT environment. A common issue with blockchain-based trading strategies is privacy disclosure. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is the primary approach to rebuilding the transaction model to address this issue [29]. Smart contracts, the differential private stochastic gradient descent technique, and system architecture and design are all implemented by [30]. To achieve the aim of secure storage and exchange of medical data, authors in [31] present a whole medical information system model based on blockchain technology. Authors in study [32] suggest a blockchain-based access control scheme called BacS for Distributed IoT. The usual approach, in which third parties obtain and manage enormous quantities of patients' Healthcare data, is called into question by the increasing rise in reported incidences of security and surveillance breaches endangering patients' privacy. Authors in the study [33], use blockchain technology to address the aforementioned problems.

Based on the related work, the research gap in IoT access control and security lies in developing a robust and privacy-preserving access control framework using blockchain technology. There is also a need to explore the potential of machine learning and deep learning algorithms for handling the massive amount of raw data generated by IoT devices. Furthermore, there is a need to address privacy and security concerns in emerging technologies such as 5G-VANET and vehicular IoT environments. The need for secure storage and exchange of medical data is also highlighted. There is a need to develop more blockchain-based access control schemes to ensure the security and privacy of data in distributed IoT environments.

5. Proposed Methodology

Fig. 1 presents a detailed methodology outlining the steps in creating a blockchain-based access control model designed to safeguard privacy in the IoT ecosystem.

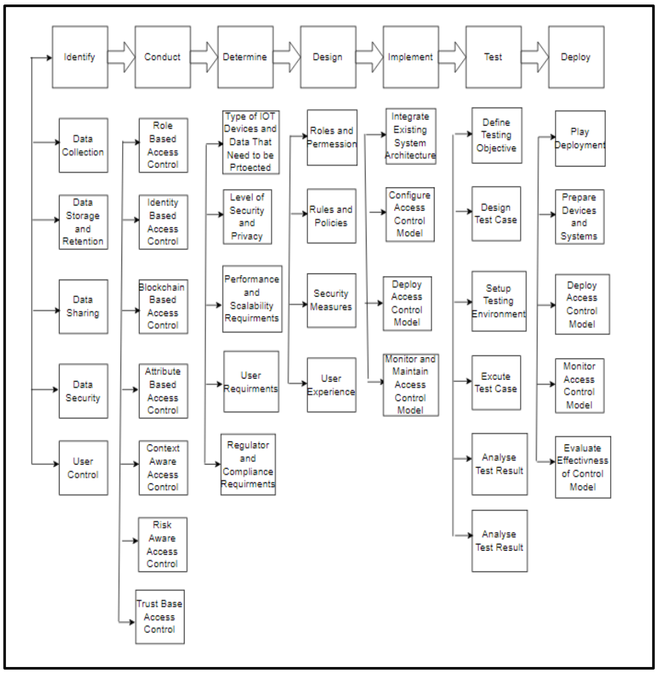
Identify
Conduct
Determine
Design
Implement
Test
Deploy
Data Collection
Data Storage and Retention
Data Sharing
Data Security
User Control
Role Based Access Control
Identity Based Access Control
Blockchain Based Access Control
Attribute Based Access Control
Context Aware Access Control
Risk Aware Access Control
Trust Base Access Control
Type of IOT Devices and Data That Need to be Prtoected
Level of Security and Privacy
Performance and Scalability Requirments
User Requirments
Regulator and Compliance Requirments
Roles and Permession
Rules and Policies
Security Measures
User Experience
Integrate Existing System Architecture
Configure Access Control Model
Deploy Access Control Model
Monitor and Maintain Access Control Model
Define Testing Objective
Design Test Case
Setup Testing Environment
Excute Test Case
Analyse Test Result
Analyse Test Result
Play Deployment
Prepare Devices and Systems
Deploy Access Control Model
Monitor Access Control Model
Evaluate Effectivness of Control Model

Fig. 1. Methodology for Access Control Model for Preserving Privacy in the IoT.

5.1. Identify

Identify the privacy risks and challenges that exist in the IoT and how they can be addressed through an access control model. There are several privacy risks and challenges that exist in the IoT that can be addressed through an access control model.

5.1.1. Data collection

The IoT involves the collection of large amounts of data from a variety of devices and sources, which can raise privacy concerns if the data is not properly protected. An access control model can help to regulate and restrict access to this data, ensuring that it is only collected and used for authorised purposes.

5.1.2. Data storage and retention

The data collected in the IoT is often stored in centralised databases or cloud systems, which can create risks if the data is not properly secured. An access control model can help to ensure that the data is only stored for as long as necessary and that access to the data is strictly controlled.

5.1.3. Data sharing

The data collected in the IoT is often shared with third parties, such as service providers or analytics firms. An access control model can help regulate and monitor this data's sharing, ensuring that it is only shared with authorised parties and for authorised purposes.

5.1.4. Data security

The data collected in the IoT is often vulnerable to security threats, such as hacking or data breaches. An access control model can help to secure the data by implementing measures such as encryption and authentication.

5.1.5. User control

Users of IoT devices may not have control over the data collected about them or how it is used. An access control model can help to give users more control over their data by allowing them to specify their privacy preferences and access rights.

5.2. Conduct

Conduct a review of the existing access control models and technologies developed for the IoT, including both centralised and decentralised approaches. Several IoT access control models and technologies have been developed, including centralised and decentralised approaches. Centralised access control models are based on a central authority regulating access to IoT resources. These models are often hierarchical in nature, with the central authority determining which parties are allowed access to which resources. Examples of centralised access control models for the IoT include the following.

5.2.1. Role-based access control (RBAC)

This model uses roles to control access to resources in the IoT. Users are assigned to specific roles based on their responsibilities, and access to resources is granted based on their roles.

5.2.2. Identity-based access control (IBAC)

This model uses identities (e.g., usernames and passwords) to control access to resources in the IoT. Access to resources is granted based on the identity of the user attempting to access the resources. Decentralised access control models are based on distributed systems that do not rely on a central authority to regulate access to resources. These models are often based on blockchain technology, enabling secure and transparent access control without a central authority.

5.2.3. Blockchain-based access control

This model uses blockchain technology to create a decentralised and secure system for managing access to resources in the IoT. Transactions on the blockchain represent access control decisions, and the blockchain is used to verify and enforce these decisions.

5.2.4. Attribute-based access control (ABAC)

This model uses attributes (e.g., user characteristics, device properties, etc.) to control access to resources in the IoT. Access to resources is granted based on the attributes of the user attempting to access the resources. Role-based Access Control (RBAC), which assigns roles to users based on their job functions, responsibilities, and permissions, and Attribute-based Access Control (ABAC), which determines access rights based on a set of user attributes, such as job title, location, and time of day, are other access control models and technologies that have been developed for the IoT. Context-aware Access Control (CAC), which takes into account contextual elements, including the user's location and the device being used when making access choices, and Rule-based Access Control (RuBAC), which employs a set of rules to establish access privileges, are further options. Access control methods for the IoT have also used biometric-based authentication technologies like fingerprint and face recognition. These concepts and technologies enable various access control strategies and may be used with blockchain-based products to increase security and privacy protection in IoT contexts.

5.2.5. Context-aware access control

This model uses context (e.g., location, time, etc.) to control access to resources in the IoT. Access to resources is granted based on the context in which the user is attempting to access the resources.

5.2.6. Risk-aware access control

This model uses risk assessment to control access to resources in the IoT. Access to resources is granted based on the risk level associated with the user attempting to access the resources.

5.2.7. Trust-based access control

This model uses trust relationships to control access to resources in the IoT. Access to resources is granted based on the trust level that is established between the user and the resources.

5.3. Determine

Determine the specific requirements and constraints of the access control model, such as the types of IOT devices and data that need to be protected, the level of security and privacy that is needed, and the performance and scalability requirements. To determine the specific requirements and constraints of an access control model for the IoT, you will need to consider several factors, such as the following.

5.3.1. Types of IoT devices and data that need to be protected

You will need to identify the specific types of devices and data that need to be protected by the access control model. This may include devices such as sensors, cameras, and smart appliances, as well as data such as user information, sensor readings, and device logs.

5.3.2. Level of security and privacy that is needed

You will need to consider the level of security and privacy that is required for the access control model. This may involve assessing the potential risks and vulnerabilities of the IoT system and determining the measures that need to be in place to protect against these risks.

5.3.3. Performance and scalability requirements

You will need to consider the performance and scalability requirements of the access control model. This may involve assessing the expected volume of access requests and the speed at which the model needs to be able to process these requests. You will also need to consider the ability of the model to scale as the IoT system grows and evolves.

5.3.4. User requirements

You will need to consider the requirements of the users of the IoT system. This may include their preferences for privacy and security, as well as their need for ease of use and accessibility.

5.3.5. Regulatory and compliance requirements

You will need to consider any regulatory or compliance requirements that apply to the access control model. This may include requirements related to data protection and privacy laws and industry-specific regulations. By considering these factors, you can develop an access control model that meets the specific needs and constraints of the IoT system.

5.4. Design

Design the access control model based on the requirements and constraints identified in step 3. This may involve defining the roles and permissions of different users and devices and the rules and policies for granting and revoking access. To design an access control model for the IoT based on the identified requirements and constraints, you will need to consider several factors, such as the following.

5.4.1. Roles and permissions

You will need to define the roles and permissions of different users and devices in the IoT system. This may involve specifying the types of actions each user or device is allowed to perform and the resources they are allowed to access.

5.4.2. Rules and policies

You will need to define the rules and policies for granting and revoking access to resources in the IoT system. This may involve specifying the conditions under which access is granted or denied and the procedures for requesting and approving access.

5.4.3. Security measures

You will need to consider the security measures that are needed to protect the access control model and the IoT system. This may involve implementing measures such as encryption, authentication, and authorisation.

5.4.4. User experience

You will need to consider the user experience of the access control model. This may involve making the model easy to use and understand and providing users with the necessary tools and resources to manage their access to resources in the IoT system. By considering these factors, you can design an access control model that meets the specific needs and constraints of the IoT system and effectively preserves privacy in the system.

5.5. Implement

Implementing the access control model in the IoT system may involve integrating the model into the existing system architecture and configuring it to control access to data according to the specified rules. To implement an access control model in the IoT system, you will need to follow the following steps.

5.5.1. Integrate the access control model into the existing system architecture

You will need to incorporate the access control model into the existing system architecture, ensuring that it is properly integrated with the other components of the system. This may involve modifying the system's database or cloud storage systems to support the model's data requirements and integrating the model with the system's security infrastructure.

5.5.2. Configure the access control model

You will need to configure the access control model to control access to data in the IoT system according to the specified rules. This may involve setting up the model's roles and permissions and defining the rules and policies for granting and revoking access.

5.5.3. Deploy the access control model

You will need to deploy the access control model in the IoT system, rolling it out to all relevant devices and systems in the system.

5.5.4. Monitor and maintain the access control model

You will need to monitor the access control model to ensure that it continues to function properly and effectively control access to data in the IoT system. This may involve regularly testing and updating the model as needed. By following these steps, you can implement an access control model in the IoT system and ensure that it effectively controls access to data in the system.

5.6. Test

Test the access control model to ensure that it functions correctly and effectively to preserve privacy in the IoT system. This may involve conducting simulations or experiments to evaluate the model's performance. To test an access control model for the IoT system, you can follow the following steps.

5.6.1. Define the testing objectives

You will need to define the objectives of the testing, such as evaluating the model's performance, verifying its functionality, or assessing its effectiveness at preserving privacy in the IoT system.

5.6.2. Design the test cases

You will need to design the test cases that will be used to test the access control model. This may involve creating test scenarios that reflect different types of access requests and conditions and defining the expected outcomes of the tests.

5.6.3. Set up the testing environment

You will need to set up the testing environment, including the devices, systems, and data that will be used in the tests.

5.6.4. Execute the test cases

You will need to execute the test cases and observe the results. This may involve interacting with the access control model and the IoT system to trigger access requests and record the results.

5.6.5. Analyse the test results

You will need to analyse the test results to determine whether the access control model is functioning correctly and effectively, preserving privacy in the IoT system. This may involve comparing the results to the expected outcomes and identifying any discrepancies or issues.

5.6.6. Report on the test results

You will need to report on the test results, including any issues that were identified and any recommendations for improving the model's performance.

5.7. Deploy

Deploy the access control model in a real-world IoT environment and monitor its performance and effectiveness over time follow steps are important.

5.7.1. Plan the deployment

You will need to plan the deployment of the access control model, including the devices and systems that will be included in the deployment, the timeline for the deployment, and any necessary resources or support.

5.7.2. Prepare the devices and systems

You will need to prepare the devices and systems that will be included in the deployment, including installing any necessary software or hardware and configuring the devices and systems to support the access control model.

5.7.3. Deploy the access control model

You will need to deploy the access control model in the real-world IoT environment, rolling it out to the devices and systems that have been prepared.

5.7.4. Monitor the performance of the access control model

You will need to monitor the performance over time to ensure that it is functioning correctly and effectively, preserving privacy in the IoT environment. This may involve tracking key performance indicators (KPIs) and collecting data on the model's usage and effectiveness.

5.7.5. Evaluate the effectiveness of the access control model

You will need to evaluate the effectiveness of the access control model in preserving privacy in the real-world IoT environment.

6. Conclusion

In conclusion, the use of blockchain technology as a basis for an access control model has the potential to preserve privacy in the Internet of Things effectively. By utilizing a decentralized, distributed ledger, blockchain can provide secure, tamper-proof storage of access control rules and user identities, ensuring that sensitive information is protected from unauthorized access. Furthermore, by using decentralized authentication, blockchain-based access control models can allow for more granular and efficient control over access to IoT resources. While further research is needed to realize the potential of this technology fully, it offers a promising solution for preserving privacy in the increasingly connected world of the IoT’s.

References

1. Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, *54*, 1-31.
2. Vermesan, O., Friess, P., Guillemin, P., Sundmaeker, H., Eisenhauer, M., Moessner, K., & Cousin, P. (2022). Internet of things strategic research and innovation agenda. In Internet of Things (pp. 7-151). River Publishers.
3. Al-Ali, A. R., Gupta, R., Zaman Batool, T., Landolsi, T., Aloul, F., & Al Nabulsi, A. (2020). Digital twin conceptual model within the context of internet of things. *Future Internet*, *12*(10), 163.
4. Pereira, F., Correia, R., Pinho, P., Lopes, S. I., & Carvalho, N. B. (2020). Challenges in resource-constrained IoT devices: Energy and communication as critical success factors for future IoT deployment. *Sensors*, *20*(22), 6420.
5. Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., ... & Doody, P. (2022). Internet of things strategic research roadmap. In *Internet of things-global technological and societal trends from smart environments and spaces to green ICT* (pp. 9-52). River Publishers.
6. Hossain, M. M., Fotouhi, M., & Hasan, R. (2015, June). Towards an analysis of security issues, challenges, and open problems in the internet of things. In *2015 ieee world congress on services* (pp. 21-28). IEEE.
7. King, N. J., & Raja, V. T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review*, *28*(3), 308-319.
8. Kushwaha, A., & Kushwaha, V. (2011). Location based services using android mobile operating system. *International Journal of Advances in Engineering & Technology*, *1*(1), 14.
9. Rathore, M. M., Ahmad, A., Paul, A., & Rho, S. (2016). Urban planning and building smart cities based on the internet of things using big data analytics. *Computer networks*, *101*, 63-80.
10. Khan, A. S., Yahya, M. I. B., Zen, K. B., Abdullah, J. B., Rashid, R. B. A., Javed, Y., ... & Mostafa, A. M. (2023). Blockchain-Based Lightweight Multifactor Authentication for Cell-Free in Ultra-Dense 6G-Based (6-CMAS) Cellular Network. IEEE Access, 11, 20524-20541.
11. Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, *92*, 101747.
12. Tellabi, A., Sassmanhausen, J., Bajramovic, E., & Ruland, K. C. (2018, July). Overview of Authentication and Access Controls for I&C systems. In *2018 IEEE 16th International Conference on Industrial Informatics (INDIN)* (pp. 882-889). IEEE.
13. Ahmed, D. M., Ameen, S. Y., Omar, N., Kak, S. F., Rashid, Z. N., Yasin, H. M., ... & Ahmed, A. M. (2021). A state of art for survey of combined iris and fingerprint recognition systems. *Asian Journal of Research in Computer Science*, 18-33.
14. Khan, N., Abdullah, J., & Khan, A. S. (2015, August). Towards vulnerability prevention model for web browser using interceptor approach. In 2015 9th International Conference on IT in Asia (CITA) (pp. 1-5). IEEE.
15. Alarfaj, F. K., & Khan, N. A. (2023). Enhancing the Performance of SQL Injection Attack Detection through Probabilistic Neural Networks. Applied Sciences, 13(7), 4365.
16. Patwary, A. A. N., Fu, A., Naha, R. K., Battula, S. K., Garg, S., Patwary, M. A. K., & Aghasian, E. (2020). Authentication, access control, privacy, threats and trust management towards securing fog computing environments: A review. *arXiv preprint arXiv:2003.00395*.
17. Kempeners, M. A., & Van der Hart, H. W. (1999). Designing account management organizations. *Journal of Business & Industrial Marketing*.
18. Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., ... & Scarfone, K. (2013). Guide to attribute based access control (abac) definition and considerations (draft). *NIST special publication*, *800*(162), 1-54.
19. Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2012). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE transactions on parallel and distributed systems*, *24*(1), 131-143.
20. Al Omar, A., Rahman, M. S., Basu, A., & Kiyomoto, S. (2017, December). Medibchain: A blockchain based privacy preserving platform for healthcare data. In *International conference on security, privacy and anonymity in computation, communication and storage* (pp. 534-543). Springer, Cham.
21. Frikha, T., Chaari, A., Chaabane, F., Cheikhrouhou, O., & Zaguia, A. (2021). Healthcare and fitness data management using the iot-based blockchain platform. *Journal of Healthcare Engineering*, *2021*.
22. Peng, S., Hu, X., Zhang, J., Xie, X., Long, C., Tian, Z., & Jiang, H. (2020). An efficient double-layer blockchain

method for vaccine production supervision. *IEEE transactions on nanobioscience*, *19*(3), 579-587.

23. Khan, A. S., Javed, Y., Saqib, R. M., Ahmad, Z., Abdullah, J., Zen, K., ... & Khan, N. A. (2022). Lightweight Multifactor Authentication Scheme for NextGen Cellular Networks. IEEE Access, 10, 31273-31288.
24. Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2016). FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Security and communication networks*, *9*(18), 5943-5964.
25. Khan, N. A., & Al Qurashi, M. (2023). Security Tradeoff in Network Virtualization and Their Countermeasures. In Inventive Computation and Information Technologies: Proceedings of ICICIT 2022 (pp. 741-749). Singapore: Springer Nature Singapore.
26. Saif, S., Biswas, S., & Chattopadhyay, S. (2020). Intelligent, secure big health data management using deep learning and blockchain technology: an overview. *Deep Learning Techniques for Biomedical and Health Informatics*, 187-209.
27. Ouaddah, A. (2019). A blockchain based access control framework for the security and privacy of IoT with strong anonymity unlinkability and intractability guarantees. In *Advances in Computers* (Vol. 115, pp. 211-258). Elsevier.
28. Xie, L., Ding, Y., Yang, H., & Wang, X. (2019). Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. *IEEE Access*, *7*, 56656-56666.
29. Guan, Z., Lu, X., Yang, W., Wu, L., Wang, N., & Zhang, Z. (2021). Achieving efficient and Privacy-preserving energy trading based on blockchain and ABE in smart grid. *Journal of Parallel and Distributed Computing*, *147*, 34-45.
30. Qashlan, A., Nanda, P., He, X., & Mohanty, M. (2021). Privacy-preserving mechanism in smart home using blockchain. *IEEE Access*, *9*, 103651-103669.
31. Alqarni, A. A., Alsharif, N., Khan, N. A., Georgieva, L., Pardade, E., & Alzahrani, M. Y. (2022). MNN-XSS: Modular neural network based approach for XSS attack detection. Computers, Materials and Continua, 70(2), 4075-4085.
32. Chen, Z., Xu, W., Wang, B., & Yu, H. (2021). A blockchain-based preserving and sharing system for medical data privacy. *Future Generation Computer Systems*, *124*, 338-350.
33. Meisami, S., Beheshti-Atashgah, M., & Aref, M. R. (2021). Using Blockchain to Achieve Decentralized Privacy In IoT Healthcare. *arXiv preprint arXiv:2109.14812*.