Journal of Computer Science & Computational Mathematics, *Volume 13, Issue 2, June 2023*
DOI: 10.20967/jcscm.2023.02.004

Comprehensive Analysis of Security Issues in Cloud-Based Internet of Things: A Survey

Usman Abdul Gimba[1,4,*], Noor Afiza Mohd Ariffin[1], Ahmad Musa[2], Lawal Babangida[3]

[1]Department of Information Security, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia
[2]Department of Computing and Cybersecurity, School of Engineering and Technology, Canterbury Christ Church University
[3]Department of Computer Science, School of Sciences, Federal College of Education, Katsina, Nigeria
[4]Department of Cyber Security, Faculty of Computing, Federal University Dutse, Jigawa, Nigeria
[*]Corresponding author email: usman_gimba@yahoo.co.uk

***Abstract*:** The Internet of Things (IoT) has emerged as the largest computing platform, enabling IoT devices to sense real-world conditions such as temperature, humidity, pressure, and cloud prediction. However, the security of IoT systems is crucial due to their direct impact on human life. With the expansion of processing and communication capabilities to numerous devices, IoT has become a vast network where connectivity is ubiquitous. This paper focuses on the security issues of cloud-based IoT, specifically access control, network security, data security, and privacy, which are the four main components of cloud-based IoT. By analyzing and comparing existing research papers on security in cloud IoT and IoT in general, we identify proposed solutions. Most researchers have concentrated on a single component, while only a few have addressed two components. Consequently, our research aims to bridge the gap in Cloud IoT security by focusing on more than two components. We propose the utilization of methods such as Machine Learning and blockchain to enhance security, drawing on the strengths highlighted in previous works. Our future focus will involve exploring potential attacks in cloud IoT and developing a comprehensive method that encompasses at least three security components of cloud IoT security.

***Keywords*:** IoT-Security, blockchain, cloud security, access control, and privacy.

1. Introduction

The Internet of Things (IoT) is a rapidly evolving technology that has experienced significant growth in recent years. IoT can be defined as a network of physical objects, such as vehicles, buildings, and devices, embedded with electronics, software, sensors, actuators, and internet connectivity to enable data gathering and exchange [1]. According to [2], IoT consists of physical objects embedded with electronics, software, and sensors, enabling remote sensing and control over existing network infrastructure. This integration of the physical world with communication networks has led to improved efficiency, accuracy, and economic benefits, finding applications in various environments such as smart houses, medical healthcare systems, smart cities, manufacturing, and transportation [3]. The expansion of computation and communication capabilities to numerous devices on a large scale has led to the adoption of cloud computing for managing the vast amount of data generated by IoT systems. The cloud model offers Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) delivery models. By processing and storing IoT data in the cloud, its effectiveness is improved[4]. However, securing IoT devices and ensuring the privacy and security of collected and transmitted data are crucial. IoT applications provide valuable services but raise concerns about privacy and security. Unlike traditional internet systems, IoT devices gather and analyze data without the need for human presence, requiring different security measures beyond traditional asymmetric key-based protocols and IP-based solutions. Figure 1 illustrates the Cloud-based IoT architecture:

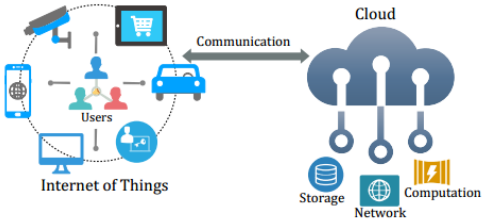

Figure 1. Cloud Based IoT Architecture[4]

Cloud computing is a promising technology with significant customer benefits, but it also presents security concerns and weaknesses. The integration of IoT and the cloud introduces opportunities to leverage cloud technologies [5]. However, it also brings new challenges, particularly in terms of security and privacy in both the cloud and IoT environments. These challenges can lead to threats such as multi-tenancy vulnerabilities, Internet protocol and browser vulnerabilities, network attacks, unauthorized access, and data disclosure [6]. This paper aims to address the security challenges in cloud-based IoT by focusing on the four main security components of access control, network security, data security and privacy. By identifying the existing gaps in cloud IoT security, researchers can better address these gaps using current methods.

2. Related works

Chaabouni et al. [7] conducted a survey on Network Intrusion Detection Systems (NIDSs) using both traditional and machine learning techniques, providing a comprehensive re-

view of NIDSs deployed in various aspects of machine learning techniques for IoT. Allifah & Zualkernan [8] presented a systematic survey of security vulnerabilities in smart home customer devices and introduced a novel methodology for systematically ranking the security of these devices. The Analytic Hierarchy Process (AHP) was employed as a general risk security ranking model, known for its robustness against pairing assumptions. Lia S. [9] focused on identifying security threats and issues in IoT, aiming to enhance users' and manufacturers' understanding of the impact of security in IoT devices. The survey respondents consisted of individuals with knowledge of data transfer in IoT devices (63%) and those with less knowledge (36.7%). Mohammad Noor [10] conducted a survey on IoT security from 2016 to 2018, examining current trends in IoT security research, tools, IoT modellers, and simulators. The survey provided an overview of IoT security research trends and highlighted relevant simulators and tools within the three-year period. Kumar et al. [11] comprehensively analyzed security mechanisms for the IoT environment, including possible security threats. The paper discussed existing security threats, proposed security mechanisms, and vulnerabilities of cloud-based IoT environments. Thabit et al. [12] conducted a survey on lightweight block cyphers, stream cyphers, and hybrid cipher algorithms used for securing the IoT. The evaluation included a comparison of the performance and robustness of these security algorithms, along with addressing security challenges, threats, and mitigation techniques in IoT. Bonkra & Dhiman [13] presented challenges related to Cloud-IoT security, with a specific focus on data privacy. The paper elaborated on securing data on the cloud-IoT platform to prevent unauthorized access and highlighted open security research concerns that require urgent attention. Doghrmachi & Ameen [14] focused their review paper on the architectural design of blockchain for the Internet of Things networks. They critically investigated IoT threats, security requirements, and challenges in IoT layered architecture, and addressed existing IoT security technologies for IoT applications, including solutions like blockchain and context awareness. Zar et al. [15] conducted an analysis of key issues related to network efficiency, security risk identification, and management. The paper analyzed the differences between cloud computing and IoT and examined key challenges in cloud IoT security. It also addressed security threats in cloud IoT and provided network policies to help build efficient networks. Mohiuddin & Almogren [16] presented a study investigating the challenges in cloud computing and strategies adapted to facilitate the transition of IoT applications to the Cloud. The paper also discussed open issues related to security challenges in cloud IoT. Naregal & Kalmani [17] conducted a study on Attribute-Based Encryption (ABE) in the cloud-based Internet of Things, specifically focusing on access control. ABE was utilized in cloud storage to provide efficient access control, considering the resource constraints of IoT devices and the need for lightweight encryption techniques. Kashyap et al. [18] conducted a review of the cloud-based Internet of Things with a focus on data security, including the architecture with different layers. The paper highlighted security issues and challenges at each layer of the cloud-based IoT architecture and proposed a new architecture design to ensure IoT security, achieving efficient performance and data privacy.

3. Cloud IoT Security Issues

IoT cloud computing, also known as cloud IoT, refers to the integration of cloud computing resources and IoT technologies. This integration aims to leverage the characteristics of cloud computing, such as high data storage capacity [18]. Although cloud computing and IoT are distinct concepts, their integration allows for mutual benefits. IoT connects the physical world with the internet, enabling smart communication between the environment and the physical world. The integration of IoT and cloud revolves around three main categories: communication, storage, and computing. IoT devices operate in various settings to achieve diverse goals. Despite the numerous advantages offered by Cloud IoT to consumers and providers, its adoption is hindered by security challenges, causing hesitation among potential users. The IoT cloud environment faces security challenges that are different from conventional cloud computing security challenges and can significantly impact the entire paradigm [19]. Ensuring the security of IoT systems is challenging due to their complexity, multidisciplinary nature, and extensive attack surface [20]. As IoT devices are connected via wireless networks and often operate in unattended environments, they become vulnerable to eavesdropping and physical access by attackers. Limited computational resources and power in IoT devices make it difficult to implement complex security structures [21]. The primary objective of IoT systems is to enable anyone, anywhere, at any time to access them [22], but this accessibility also presents opportunities for attackers to exploit and gain unauthorized access to files [21]. The security issues in Cloud IoT encompass IoT technology security [23] cloud security [24], and IoT cloud architecture security.

The increasing misuse of computer systems and threats to personal privacy have sparked interest in implementing technical measures for data protection [25]. The security issues in cloud IoT can be categorized into four components: access control, network security, data security, and privacy. Access control is implemented to restrict users' access to data sets outside their jurisdiction, ensuring that they can only read from or write to specific data sets, thus preventing security breaches [25–27]. Data security involves safeguarding digital data from unauthorized access by cyber attackers or data breaches, which entails using encryption algorithms. Data security in cloud storage focuses on data confidentiality, integrity, and availability [28–30]. Network security encompasses policies and procedures for protecting devices, ensuring confidentiality, integrity, and authentication to prevent, detect, and monitor unauthorized use of network resources (via intrusion detection systems or firewalls) [31, 32]. Privacy schemes control the collection, use, and sharing of personal information on the internet, aiming to keep this information safe from unauthorized use, theft, or loss [33–35].

3.1 Network Security

IoT security can be defined as a set of cybersecurity strategies and protection mechanisms designed to safeguard network-connected IoT devices against cyberattacks. In order to ensure IoT security, it is crucial to identify and halt anomalous and malicious traffic within the network. Attacks such as malware, DoS, and DDoS pose significant threats to the IoT network. Choudhary and Kesswani [36] proposed the Key Match Algorithm (KMA) and Cluster-Based Algorithm (CBA) to detect and prevent routing attacks. The KMA demonstrated a true positive intrusion detection rate ranging from 50% to 80%, while the CBA showed a rate of 76% to 96%. Sugi and Ratna [37] explored the use of Long-Short-Term Memory (LSTM) and K-Nearest Neighbor (KNN) algorithms for intrusion detection. These machine learning and deep learning algorithms were utilized to develop an attack detection model. Shafiq et al. [38] introduced the CorrAUC, which is based on a wrapper technique for accurate feature selection and effective feature representation for ML algorithms. Topsis and Shannon entropy, based on bijective soft set, were integrated to validate the selected features for identifying malicious traffic, achieving a result exceeding 96%. Alam [39] proposed a new framework called MANET for establishing secure and effective connectivity between smart devices. MANET addresses communication challenges in 5G networks among smart devices. Toth and Chowdhury [40] suggested the incorporation of honeynets into cloud service provider networks to enhance the accuracy of intrusion detection systems and analyze attack vectors used by attackers, thereby improving security control. Aghili et al. [41] introduced the Secure and Lightweight Mutual RFID Authentication (SecLAP) protocol to ensure secure communication and maintain privacy in Medical IoT. The results indicate that SecLAP consumes fewer resources, computational functions, and network flows compared to previous techniques.

Table 1. Related works on Network Security

Author	Proposed solution	Opinion/critic
[36]	Key match algorithm and cluster-based algorithm to detect and prevent routing attack	Only two attacks were investigated and there are many attacks possible, in my opinion, more attacks should have been selected to prevent those attacks from happening. However, it only simulated the proposed method and was not used in a practical Cloud IoT environment.
[37]	IDS based on ML and DL using LSTM and KNN algorithm to overcome security attacks in IoT network	The algorithms could detect attacks, but however, the proposed algorithm was only simulated, it was not used in a practical environment to show its full functionality.
[38]	Feature selection algorithm based on machine learning	In my opinion time complexity should be included in the research to ease the algorithm in detection.
[39]	Proposed MANET as a new framework for an effective and secure smart device to smart device connectivity	This will increase the security in 5G networks, but it should have been tested in a real application to get a better result.
[41]	Proposed a solution by in-cooperating honeynets into the cloud network to prevent information leakages and hardening of an information system against unauthorized individuals.	The paper focuses only on honeypots and honeynet to improve the security, the authors need to broaden their scope to show other algorithms that can be used to improve the security.
[40]	Proposed SecLAP to provide secure communication and privacy of Medical IoT systems and medical data. The SecLAP protocol can prevent many types of network attacks	Theoretically, the proposed SecLAP is secure, but the authors could not apply it in real-world Medical IoT to show an accurate real-world result.

3.2 Data Security

Data security risks primarily arise when data is transferred, stored, and processed in clouds that are external to the user's network and are owned by third parties. These risks can be classified into two categories: data loss, which refers to the destruction of consumer data, and data breach, which refers to unauthorized individuals gaining access to consumer data. Several researchers have proposed approaches to address data security. Midi et al. [42] presented Kalis, a self-adapting, knowledge-driven intrusion detection system capable of real-time attack detection in IoT systems. Kalis does not require any modifications to IoT software, supports a wide range of protocol monitoring, and has no impact on the performance of IoT device applications. Rebbah et al. [43] proposed a signature-based intrusion detection system for the cloud IoT environment. This IoT security approach effectively mitigated intrusion detection by calculating temporary and spatial user profiles based on data requests.

Mollah et al. [44] introduced a lightweight cryptographic scheme for secure data sharing and searching in IoT smart devices. The scheme utilizes AES, RSA, and SHA-256 for encryption and hash functions, reducing computation and communication overhead. Chen et al. [45] proposed a Security Gateway Application (SGA) that employs lightweight symmetric key cryptographic techniques and key exchange for secure end-to-end and machine-to-machine communication. SGA provides a mutual authentication mechanism and safeguards against several guessing attacks. Wu et al. [46] presented a scheme featuring multiple authorization centers and fixed-length ciphertext policy attribute encryption. The scheme improved the speed of encryption and decryption while reducing time costs, as demonstrated using the Diffie-

Hellman hypothesis.

Asare et al. [47] suggested a hybrid cryptographic algorithm to prevent unauthorized access to data transmitted between nodes in IoT. Twofish and Diffie-Hellman key exchanges are employed to ensure data security during node-to-node communication. Faika et al. [48] proposed a novel wireless battery management system architecture that incorporates blockchain technology. This architecture enhances secure communication in IoT wireless battery management systems and ensures data security to prevent cyberattacks.

3.3 Access Control

Access control in the IoT network refers to the permissions granted to users for resource usage. It can be classified into two categories: data holder and data collector. Data holders, which include users and things, provide data to the data collector, and the data collector must be able to authenticate the data holder from whom the information is collected. Li [4] proposed a novel framework for assessing the security and reputation of cloud services by integrating security-based and reputation-based trust assessment methods. The experiment conducted demonstrated that this framework outperforms state-of-the-art trust assessment methods. Mahalle [49] introduced the Identity Authentication and Capacity-based Access Control (IACAC) model to prevent unauthorized access. The IACAC effectively safeguards the IoT against attacks such as man-in-the-middle, replay, and denial of service (DoS). Evaluation using a security protocol verification tool confirmed its efficacy. Park and Sandhu [50] proposed the UCONABC control model, which encompasses traditional access control, trust management, and digital rights management. This model simplifies the control of user access and can be utilized for next-generation access control systems.

Alshehri et al. [51] presented the DSA-Block model, which utilizes blockchain technology for dynamic secure access control, enabling secure data sharing and access control. The PBFT consensus algorithm was employed for access control, and the proposed DSA-Block model exhibited improved performance compared to previous approaches. Gupta et al. [52] introduced the Google Cloud Platform Access Control (GCPAC) model to bridge the gap between real-world cloud IoT systems and access control models. The GCP-IoTAC model, an extension of GCPAC, was developed with IoT components in mind. Ren et al. [53] proposed a scheme using Cipher Policy Attribute-Based Encryption (CP-ABE) to strengthen encryption before access control. The CP-ABE scheme significantly reduces computation costs in IoT environments

3.4 Privacy

Privacy refers to the protection of information from unauthorized disclosure at all levels. The vast amount of information held by the IoT, accessible remotely, underscores the importance of privacy protection. Information leaks and unauthorized manipulation are inherent aspects of privacy, and without a trusted and interoperable IoT ecosystem, new IoT applications may fail to realize their full potential. Li et al. [54] utilized identity-based signatures to propose an efficient Message Authentication with Enhanced Privacy (IMAEP) scheme. This scheme exhibits lower computational overhead and unconditional privacy compared to

Table 2. Related works on Data Security

Author	Proposed solution	Opinion/critic
[42]	Self-adapting, knowledge-driven intrusion detection system for real-time attack detection	For the more accurate result of IDS, machine learning technique should be used because it combines both knowledge modelling and collective knowledge. This paper only chose knowledge-based for the IDS.
[43]	Intrusion detection using the signature-based approach to curb intrusion in cloud IoT	the paper should have also addressed prevention so that after detection it will prevent it from happening again, and also the efficiency of detection should have been shown.
[44]	Data sharing and searching scheme in IoT smart devices.	Only efficiency was tested but accuracy is also important in data sharing.
[45]	Lightweight symmetric key cryptographic and key exchange for secure M2M	More attacks should be looked at, the researchers should look more into other attackers to prevent those attacks.
[46]	Proposed a scheme with a multi-authorization centre and fixed-length ciphertext policy attribute encryption. The scheme improves data storage security and access control flexibility.	The paper improves data security and access control with increased efficiency and increases security to prevent unauthorized access.
[47]	Proposed a hybrid cryptographic algorithm to prevent unauthorized access to data between nodes in IoT. Using Twofish and DHE to ensure data security when communicating between nodes.	The paper ensures data security. However, the reasons for the chosen algorithms were not clearly stated a comparison with other algorithms was not done to prove how effective the Twofish and DHE are.
[48]	Proposed blockchain technology to ensure secure communication in the IoT wireless battery management systems and data security to prevent cyber-attacks.	The proposed method will increase the security against cyber-attacks; however, the cybersecurity framework should be presented comprehensively.

Table 3. Related works on Access Control

Author	Proposed solution	Opinion/critic
[4]	Novel trust assessment framework for cloud service security using trust assessment methods reputation-based and security-based	Simulation of the proposed framework validates the performance and availability. However, it was not practically used in a cold environment.
[49]	An Identity Authentication and Capacity based Access Control (IACAC) model was proposed to prevent unauthorized access	The accuracy of the proposed model in access control policy isn't addressed
[50]	Decision factors Authorization, Obligations and Conditions	Authentication, confidentiality is part of access control, and they were not addressed in this paper
[51]	Proposed a blockchain (DSA-Block) model to propose dynamic secure access control	In cooperating blockchain into the IoT will enhance the security thereby, making it more difficult to bypass without authorization.
[52]	Proposed Google Cloud Platform (GCPAC) model to bridge the gap between real-world cloud IoT and access control models	The proposed scheme will prevent lots of attacks like insider attacks, guess password attacks etc. and this will make the system secure from unauthorized access.
[53]	Proposed a scheme that uses cypher policy attributes-based encryption to increase flexibility and robustness of access control. The general framework to solve the security requirement is described in the scheme.	The result of comparison with other schemes was not presented to show how this scheme is better than the previously proposed schemes.

similar-level schemes. Arabo [55] proposed a context-based dynamic cloud security framework to address issues related to smart/mobile devices and cloud services. The framework includes a dynamic secure cloud resilience framework that prevents security threats to data on smart devices. Jebri et al. [56] developed a secure generic model to ensure data secrecy, anonymity, and trust in IoT and Wireless Sensor Networks between nodes. The design incorporates Identity-Based Encryption, Pseudonym-Based Encryption, and a lightweight key agreement protocol, enhancing security and privacy compared to previously proposed solutions. Al-Turjman et al. [57] proposed a seamless secure authentication and key agreement (S-SAKA) for secure user authentication in cloud-based environments. The S-SAKA approach is resistant to various attacks and reduces computational and communication costs compared to previous solutions. Lee et al. [58] identified identity and password guessing, replay, and session key disclosure attacks as vulnerabilities in Sharma and Kalra's multi-factor authentication scheme. The newly proposed secure multifactor authentication protocol resolves all the identified attacks in Sharma and Kalra's scheme. Tawalbeh et al. [59] introduced new IoT layered models that incorporate identification, privacy, and security components. These models facilitate secure data transfer between the layers, supported by a certificate of security.

4. Discussion

The survey component can be conducted based on access control, data security, network security, and privacy. The summary of each component is described in Tables 1, 2, 3 and 4, respectively. These tables provide an explanation of the previous works proposed by researchers and the methods they used to achieve results in their papers. Table 5 compares the proposed solutions for cloud-IoT security based on the four major security components. The purpose of this comparison is to assess the strength of the proposed solutions against the security issues in Cloud-IoT. The choice of algorithms used determines the ability to securely prevent unauthorized access to smart devices in the IoT. Machine learning, deep learning, and blockchain techniques have proven to deliver better accuracy and efficiency in securing cloud-based IoT. However, the previously proposed solutions have not adequately addressed all four security components. Most solutions only address one security issue, leaving vulnerabilities in other areas. Based on the survey, it was observed that size, weight, user interface, comfortability, and battery/power consumption are factors influencing IoT deployment.

IoT researchers and developers must select a secure cloud-IoT platform. A good cloud-based IoT platform should include security measures such as authentication, reliability, confidentiality, and integrity. The four security components should be the main considerations when choosing a cloud-IoT platform. If a platform can guarantee the security of these components, it can be deemed suitable for the client. According to Table 5, [37] and [38] demonstrate higher accuracy in detecting attacks related to network security and privacy, while [50] and [51] perform better in terms of access control and data security. To enhance cloud-IoT security, it is necessary for the proposed solutions to address security issues across all four components. Combining the approaches of [37], [38], [50], and [51] could lead to a new security scheme that effectively protects the Cloud-IoT environment across all four components.

5. Conclusion

The widespread deployment of IoT devices and their integration with the cloud highlight the critical importance of securing these devices to protect both the physical and cyber

Table 4. Related works on Privacy

Author	Proposed solution	Opinion/critic
[4]	Novel trust assessment framework for cloud service security using trust assessment methods reputation-based and security-based	Simulation of the proposed framework validates the performance and availability. However, it was not practically used in a cold environment.
[55]	Context-based dynamic framework for cloud security The paper addressed the privacy issue connected to mobile devices.	However, it was theoretical the proposed solution was not tested in a real environment to prove its full functionality.
[56]	Secure generic model based on lightweight key agreement protocol, the Identity-Based Encryption and Pseudonym Based Encryption	However, the proposed solution was not tested on real environment or simulated to show how its full functionality.
[57]	Seamless secure authentication and key agreement approach based on bilinear pairing and elliptic-curve cryptosystem	User authentication should have been considered because privacy starts from the user, making sure that the user is really who he says he is.
[58]	Proposed a multifactor authentication protocol to solve the security problems like identity and password guessing, replay and session key disclosure attacks. These attacks are among the attacks bothering cloud IoT and preventing them will increase the security of authentication.	The proposed authentication protocol reduces unauthorized access, however, only Sharma and Kaira's schemes were taken into consideration by the authors.
[59]	Proposed new IoT layered models with layers of identification, privacy and security component. A certificate of security for secure data transfer between layers of the proposed IoT layer models.	However, a cryptographic security method capable of operating on IoT devices and standardized data collection should have been looked into.

Table 5. Comparison of solution in Cloud-based IoT security

Author	Methods	Access control	Privacy	Data sec.	Network sec.
[36]	Key Match, Cluster-Based Algorithms	o	o	o	High
[37]	LSTM, K-NN techniques (ML, DL)	o	High	Med.	High
[38]	MLAlgorithm	Med.	Low	Low	High
[39]	Markov Model, Viterbi algorithm	o	Medium	o	High
[40]	Honeynets	o	o	o	High
[41]	BAN logic, FPGA	o	Medium	o	High
[42]	Hybrid signature/anomaly-based	o	o	High	o
[43]	Signature-based approach	o	o	o	High
[44]	AES, RSA, SHA-256	o	o	High	Med.
[45]	Cryptographic symmetric key algorithm	Med.	o	High	o
[46]	CP-ABE	High	o	High	o
[47]	Diffie-Hellman key exchange, TwoFish algorithm	o	o	High	Medium
[48]	Blockchain, Hyperledger-Fabric	High	Med.	High	Low
[49]	IACAC model	High	Med.	o	o
[50]	UCONABC model	High	o	o	o
[51]	Blockchain (DSA-Block) model	High	Low	Med.	Medium
[52]	GCP-IoTAC model	High	o	o	o
[53]	cipher policy attributes-based encryption	High	Low	o	o
[54]	Identity based signature	o	High	o	o
[56]	Key agreement protocol, (IBE), PBC	o	High	Medium	o
[57]	Bilinear Pairing and elliptic-curve cryptosystems	o	High	Low	o
[58]	Sharma and Kalra scheme, biometric	o	High	o	o

worlds. In this survey, our research has focused on presenting the security issues related to cloud-based IoT. The identified security issues encompass network security, data security, access control, and privacy, which emerge as the main concerns in cloud IoT based on the reviewed literature. Furthermore, the paper discusses the solutions proposed by previous researchers, providing insights and constructive criticism on how to enhance the security of cloud-based IoT. In our future research, we aim to develop methods for detecting attacks in

cloud IoT and compare them with the solutions proposed by previous researchers to identify the most effective methodology. Additionally, we plan to propose a comprehensive model that addresses attacks while enhancing privacy, data security, network security, and access control. This model will serve as a framework to mitigate the identified security challenges in cloud-based IoT, ensuring a robust and secure environment for IoT deployments.

References

[1] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[2] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and Privacy for Cloud-Based IoT: Challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017.

[3] G. Verma and S. Prakash, "A Study towards Current Trends, Issues and Challenges in Internet of Things (IoT) based System for Intelligent Energy Management," *2019 4th International Conference on Information Systems and Computer Networks, ISCON 2019*, pp. 358–365, 2019.

[4] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, and D. Chen, "Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach," *IEEE Access*, vol. 7, no. c, pp. 9368–9383, 2019.

[5] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, "Secure integration of IoT and Cloud Computing," *Future Generation Computer Systems*, vol. 78, no. December 2017, pp. 964–975, 2018. [Online]. Available: http://dx.doi.org/10.1016/j.future.2016.11.031

[6] A. D. Wankhade and K. Wagh, "A Survey on Security Challenges and Defending Methods in Cloud Based Internet of Things Network," *Proceedings - 2021 3rd International Conference on Advances in Computing, Communication Control and Networking, ICAC3N 2021*, pp. 1414–1417, 2021.

[7] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019.

[8] N. M. Allifah and I. A. Zualkernan, "Ranking Security of IoT-Based Smart Home Consumer Devices," *IEEE Access*, vol. 10, pp. 18 352–18 369, 2022.

[9] S. Lia, "The Internet of Things (IoT): Privacy and Security Challenges and Discovering IoT Risks through Exploratory Research," *Utica University ProQuest Dissertations Publishing*, no. 8.5.2017, pp. 2003–2005, 2022. [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/autism-spectrum-disorders

[10] M. binti Mohamad Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Computer Networks*, vol. 148, pp. 283–294, 2019. [Online]. Available: https://doi.org/10.1016/j.comnet.2018.11.025

[11] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Computer Science Review*, vol. 33, pp. 1–48, 2019. [Online]. Available: https://doi.org/10.1016/j.cosrev.2019.05.002

[12] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, "Cryptography Algorithms for Enhancing IoT Security," *Internet of Things (Netherlands)*, vol. 22, no. March, p. 100759, 2023. [Online]. Available: https://doi.org/10.1016/j.iot.2023.100759

[13] A. Bonkra and P. Dhiman, "IoT Security Challenges in Cloud Environment," *Proceedings - 2021 2nd International Conference on Computational Methods in Science and Technology, ICCMST 2021*, pp. 30–34, 2021.

[14] D. F. Doghramachi and S. Y. Ameen, "IoT Threats and Solutions with Blockchain and Context-Aware Security Design: A Review," *International Conference of Modern Trends in ICT Industry: Towards the Excellence in the ICT Industries, MTICTI 2021*, 2021.

[15] S. Zar, S. M. M. Gilani, A. R. Riaz, R. M. Abbasi, and I. Hameed, "Evolution of IoT in Cloud Computing: Risk Analysis and Potential Solutions," *Proceedings - 2021 IEEE 4th International Conference on Computing and Information Sciences, ICCIS 2021*, 2021.

[16] I. Mohiuddin and A. Almogren, "Security Challenges and Strategies for the IoT in Cloud Computing," *2020 11th International Conference on Information and Communication Systems, ICICS 2020*, pp. 367–372, 2020.

[17] K. Narezal and V. Kalmani, "Study of lightweight ABE for cloud based IoT," *Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020*, pp. 134–137, 2020.

[18] N. Kashyap, A. Rana, V. Kansal, and H. Walia, "Improve Cloud Based IoT Architecture Layer Security - A Literature Review," *Proceedings - IEEE 2021 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS 2021*, pp. 772–777, 2021.

[19] N. Almolhis, A. Mujawib Alashjaee, S. Duraibi, F. Alqahtani, and A. Nour Moussa, "The Security Issues in IoT- Cloud: A Review Nawaf," *IEEE International Colloquium on Signal Processing & its Applications*, vol. 6, no. 3, pp. 191–196, 2020.

[20] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[21] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65–88, 2015.

[22] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[23] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018. [Online]. Available: https://doi.org/10.1016/j.future.2017.11.022

[24] R. Kumar, P. Kumar, and V. Singhal, "A Survey: Review of Cloud IoT Security Techniques, Issues, and Challenges," *SSRN Electronic Journal*, 2019.

[25] D. E. Denning and P. J. Denning, "Data Security," *ACM Computing Surveys (CSUR)*, vol. 11, no. 3, pp. 227–249, 1979.

[26] W. Tolone, G. J. Ahn, T. Pai, and S. P. Hong, "Access control in collaborative systems," *ACM Computing Surveys*, vol. 37, no. 1, pp. 29–41, 2005.

[27] R. S. Sandhu and P. Samarati, "Access control: constrains what a user can do directly, as well as what programs executing on behalf of the users are allowed to do. In this way access control seeks to prevent activity that could lead to breach of security." *IEEE Communications Magazine*, vol. 32, no. September, pp. 40–48,

1994.
[28] R. Velumadhava Rao and K. Selvamani, "Data security challenges and its solutions in cloud computing," *Procedia Computer Science*, vol. 48, no. C, pp. 204–209, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.procs.2015.04.171
[29] V. Kumar, S. Chaisiri, and R. Ko, "Data security in cloud computing," *Data Security in Cloud Computing*, pp. 1–308, 2017.
[30] P. Yang, N. Xiong, and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," *IEEE Access*, vol. 8, pp. 131 723–131 740, 2020.
[31] G. A. Marin, "Network security basics," *IEEE Security and Privacy*, vol. 3, no. 6, pp. 68–72, 2005.
[32] X. Song, W. Jiang, X. Liu, H. Lu, Z. Tian, and X. Du, "A Survey of Game Theory as Applied to Social Networks," *Tsinghua Science and Technology*, vol. 25, no. 6, pp. 734–742, 2020.
[33] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Y. L. Tian, A. Ekin, J. Connell, C. F. Shu, and M. Lu, "Enabling video privacy through computer vision," *IEEE Security and Privacy*, vol. 3, no. 3, pp. 50–57, 2005.
[34] W. H. Ware, "Security and privacy in computer systems," *AFIPS Conference Proceedings - 1967 Spring Joint Computer Conference, AFIPS 1967*, pp. 279–282, 1967.
[35] P. M. Chanal and M. S. Kakkasageri, "Security and Privacy in IoT: A Survey," *Wireless Personal Communications*, vol. 115, no. 2, pp. 1667–1693, 2020. [Online]. Available: https://doi.org/10.1007/s11277-020-07649-9
[36] S. Choudhary and N. Kesswani, "Detection and Prevention of Routing Attacks in Internet of Things," *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, pp. 1537–1540, 2018.
[37] S. S. Swarna Sugi and S. R. Ratna, "Investigation of machine learning techniques in intrusion detection system for IoT network," *Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020*, pp. 1164–1167, 2020.
[38] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3242–3254, 2021.
[39] T. Alam, "Internet of Things: A Secure Cloud-based MANET Mobility Model," *SSRN Electronic Journal*, vol. 2020, pp. 1–7, 2020.
[40] E. M. Toth and M. M. Chowdhury, "Honeynets and Cloud Security," *2022 IEEE World AI IoT Congress, AIIoT 2022*, pp. 270–275, 2022.
[41] S. F. Aghili, H. Mala, P. Kaliyar, and M. Conti, "SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT," *Future Generation Computer Systems*, vol. 101, pp. 621–634, 2019. [Online]. Available: https://doi.org/10.1016/j.future.2019.07.004
[42] D. Midi, A. Rullo, A. Mudgerikar, and E. Bertino, "Kalis - A System for Knowledge-Driven Adaptable Intrusion Detection for the Internet of Things," *Proceedings - International Conference on Distributed Computing Systems*, pp. 656–666, 2017.
[43] M. Rebbah, D. El Hak Rebbah, and O. Smail, "Intrusion detection in Cloud Internet of Things environment," *Proceedings of the 2017 International Conference on Mathematics and Information Technology, ICMIT 2017*, vol. 2018-Janua, pp. 65–70, 2017.
[44] M. B. Mollah, A. K. Azad, and A. Vasilakos, "Secure data sharing and searching at the edge of cloud-assisted internet of things," *IEEE Cloud Computing*, vol. 4, no. 1, pp. 34–42, 2017.
[45] H. C. Chen, I. You, C. E. Weng, C. H. Cheng, and Y. F. Huang, "A security gateway application for End-to-End M2M communications," *Computer Standards and Interfaces*, vol. 44, pp. 85–93, 2016. [Online]. Available: http://dx.doi.org/10.1016/j.csi.2015.09.001
[46] Y. Wu, C. Wu, J. Hou, Z. Zhu, and M. Huang, "Cloud-Supported Internet of Things Data Security and Access Control in Smart Grid," pp. 764–769, 2019.
[47] B. T. Asare, K. Quist-Aphetsi, and L. Nana, "Secure data exchange between nodes in IoT using TwoFish and DHE," *Proceedings - 2019 International Conference on Cyber Security and Internet of Things, ICSIoT 2019*, pp. 101–104, 2019.
[48] T. Faika, T. Kim, J. Ochoa, M. Khan, S. W. Park, and C. S. Leung, "A Blockchain-Based Internet of Things (IoT) Network for Security-Enhanced Wireless Battery Management Systems," *2019 IEEE Industry Applications Society Annual Meeting, IAS 2019*, pp. 27–32, 2019.
[49] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (IACAC) for the internet of things," *Journal of Cyber Security and Mobility*, vol. 1, no. 4, pp. 309–348, 2012.
[50] J. Park and R. Sandhu, "The usage control model," *ACM Transactions on Information and System Security*, vol. 7, no. 1, pp. 128–174, 2004. [Online]. Available: http://doi.acm.org/10.1145/984334.984339
[51] S. Alshehri, O. Bamasaq, D. Alghazzawi, and A. Jamjoom, "Dynamic Secure Access Control and Data Sharing Through Trusted Delegation and Revocation in a Blockchain-Enabled Cloud-IoT Environment," *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 4239–4256, 2022.
[52] D. Gupta, S. Bhatt, M. Gupta, O. Kayode, and A. S. Tosun, "Access Control Model for Google Cloud IoT," *Proceedings - 2020 IEEE 6th Intl Conference on Big Data Security on Cloud, BigDataSecurity 2020, 2020 IEEE Intl Conference on High Performance and Smart Computing, HPSC 2020 and 2020 IEEE Intl Conference on Intelligent Data and Security, IDS 2020*, pp. 198–208, 2020.
[53] W. Ren, Y. Ren, M. E. Wu, and C. J. Lee, "A Robust and Flexible Access Control Scheme for Cloud-IoT Paradigm with Application to Remote Mobile Medical Monitoring," *Proceedings - 2015 3rd International Conference on Robot, Vision and Signal Processing, RVSP 2015*, pp. 130–133, 2016.
[54] J. Li, Z. Zhang, L. Hui, and Z. Zhou, "A Novel Message Authentication Scheme with Absolute Privacy for the Internet of Things Networks," *IEEE Access*, vol. 8, pp. 39 689–39 699, 2020.
[55] A. Arabo, "Privacy-aware IoT cloud survivability for future connected home ecosystem," *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, vol. 2014, pp. 803–809, 2014.
[56] S. Jebri, M. Abid, and A. Bouallegue, "An efficient scheme for anonymous communication in IoT," *Proceedings of the 2015 11th International Conference on Information Assurance and Security, IAS 2015*, pp. 7–12, 2016.
[57] F. Al-Turjman, Y. Kirsal Ever, E. Ever, H. X. Nguyen, and D. B. David, "Seamless Key Agreement Framework for Mobile-Sink in IoT Based Cloud-Centric Se-

cured Public Safety Sensor Networks," *IEEE Access*, vol. 5, pp. 24 617–24 631, 2017.

[58] J. Y. Lee, M. H. Kim, S. J. Yu, K. S. Park, and Y. H. Park, "A secure multi-factor remote user authentication scheme for Cloud-IoT applications," *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, vol. 2019-July, pp. 2–3, 2019.

[59] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," *Applied Sciences (Switzerland)*, vol. 10, no. 12, pp. 1–18, 2020.