International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Review on Cyber Security Issues in IOT-Based Cloud Computing

Dr. Awatef Salem Balobaid[1], Sameena Shaik *[2], Sangeetha Komandur[3]

Submitted: 18/09/2023 **Revised**: 19/11/2023 **Accepted**: 29/11/2023

Abstract: With the flexible architecture that cloud computing provides, data along with resources may be distributed across numerous diverse places as well as accessed by different industries. As well, the internet of things (IoT) has pointedly upgraded since cloud computing was combined. Cloud computing is becoming a viable technological and financial option for supporting both real-time along with non-real-time data in an IoT environment. However, the cloud rapid shift brought up a several security issues. Old security actions don't instantly spread over to cloud-rooted systems along with can be inadequate. The online monitoring of security attacks is addressed in this work, and several machines learning along with deep learning algorithms. Additionally, a few cryptographic-related authentication methods are explored. This paper identifies key research needs in the IoT-based cloud architecture after presenting the technological obstacles noted in the earlier studies. This paper presents future research prospects to avoid and mitigate cybersecurity risks in cloud computing based on the review completed.

Keywords: *Cloud computing; IoT; security; cybersecurity, authentication*

1. Introduction

This research discusses the security as well as administration problems with both cloud computing (CC) along with big data (BD) transferred from the IoT. This work then discusses how CC benefits IoT-based BD in order to close a knowledge break in the area of their integration with respect to security as well as privacy [1]. However, by fusing IoT technologies with CC, their development may be accelerated. IoT Cloud, often known as Cloud IoT, is a new branch of computing as a result. In other words, the cloud infrastructure stores and processes the data acquired by IoT technologies, relieving them of the problem of limited resources [2]. One of the biggest problems is security as IoT-linked devices carry on to expand quickly. Owing to online devices, the clever grid is exposed to serious attacks. An IoT-based clever grid provides the biggest attack surface for an IoT cyberattack since it comprises multiple nodes [3].

Several security issues along with challenges were raised as a result of the fast switch to the cloud. In spite of the frequent practice as well as dissemination of numerous cyber weapons, problems along with security issues with cloud platforms have been lectured during the last three years. In order to solve industrial security concerns in the cloud, deep learning (DL) has undergone rapid growth in artificial intelligence (AI) [4].

A diverse united network resource managing method rooted on data security transmission is proposed [5] as a solution to the problems with big mistakes and bad security in the IoT as well as in the traditional information transmission mechanisms based on CC. Amid further security problems, dependable device-to-device Among direct connection is a vital study part in the IoT sensor cloud system application. Through a secure joining among two IoT devices without the need for a medium agent, the access control mechanism may assure dependability. It principally calls for a two-pronged method that involves mutual authentication along with the creation of session keys [6].

Although machine learning (ML) methods may be effective in securing CC networks, there are still issues that must be resolved before they are widely used. Researchers as well as practitioners may create further effective techniques for securing their systems in a world that is becoming more linked by having a better understanding of the promise and limits of ML approaches to network security. By using ML methods, network security for big data in CC may be improved. ML algorithms may examine big amounts of data to look for patterns, oddities, along with potential security risks [7]. A framework that depicts deciding on the IoT cloud as an MCDM difficulty presents an optimal efficacy solution with an emphasis on user-specific priorities to develop particular solutions for volatile user demands along with agile market trends with their desires [8]. This framework uses an optimized distance-based approach (DBA) supported by fuzzy set theory. The rest organization is as follows Section 2 reviews some IoT cloud computing security issues and section 3 concludes the work.

[1] *Assistant Professor,* [2,3] *Lecturer*
Department Of Computer Science, College Of Computer Science & Information Technology, Jazan Univeristy, Jazan-45142, SaudiArabia
[1]*abalobaid@jazanu.edu.sa*
[2]* *Corresponding Author Email: saresearch22@gmail.com*
[3] *skomandur@jazanu.edu.sa*

2. Literature Review

This section reviews some IoT based cloud attack security, Denial of Service (DoS) attack, spoofing attack, port scanning attack, botnet attack and other security issues in cloud. Also, some of the approaches are reviewed in the table 1.

2.1. IoT based cloud attack Security in IoT-Based Cloud Computing

Yu et al. [9] shows that their plan has significant security flaws. A DoS attack might compromise the scheme. We provide a better authentication as well as key agreement system for an IoT-based CC environment to address these issues. There was informal security analysis, automatic security verification (ProVerif), and BAN-logic verification. The findings demonstrate the security and robustness of our approach against all known threats.

Zhou et al. [10] provide an authentication method for cloud servers and IoT-based infrastructures. In order to achieve the highest efficiency, the authentication method uses lightweight crypto-modules like the one-way hash function along with exclusive-or action. It not only lessens the computational strain but also qualifies the proposed approach for items with restricted resources, such sensors or IoT gadgets. The formal verification that Proverif offers ensures the proposed authentication scheme's security robustness.

Wang et al. [11] highlights a IoT-based CC authentication mechanism. This offers a three-factor authentication system that makes use of chaotic maps. The Diffie-Hellman key exchange based on Chebyshev chaos is employed to establish the session key. The session key also comprises a long-term secret. It guarantees that the system is safe from any potential session key disclosure threats. Additionally, this strategy properly updates local user passwords. It offers mutual authentication as well as session key agreement, according to a logical proof. By employing the random oracle model, the recognized study demonstrates the semantic security of the system.

Martínez-Peláez et al. [12] claim that their protocol is safe and can withstand widely used attacks. However, when assessed the protocol, the work discovered certain flaws and security vulnerabilities that rendered the system vulnerable. In order to improve security, this work makes the login, mutual authentication, and key agreement stages. Additionally, a section called "evidence of connection attempt" that shows that both the server and the user were involved. The approach improves on earlier efforts by meeting security standards and withstanding well-known threats.

2.2 Denial of service attack Security in IoT-Based Cloud

Computing

Salim et al. [13] discusses several detection and mitigation techniques that are only applicable to attacks on the cloud environment, such as distributed DoS (DDoS) attacks on all-purpose servers along with botnet attacks. The IoT layer, or cloud layer, is the focus of current surveys. A thorough approach was made with this study, including both generic DDoS attack motives as well as precise motives why invaders use IoT devices for DDoS attacks. The tools for deploying botnet-defected IoT devices for DDoS attacks on the cloud layer, along with several attack techniques to compromise IoT devices are described.

Syed et al. [14] provide an application-layer DoS attack discovery background for the Message Queuing Telemetry Transport (MQTT) protocol. The system was evaluated using real-world, protocol-compliant DoS attack scenarios. A ML -based discovery framework was created for the MQTT protocol to defend the MQTT message brokers against such attacks.

Velliangiri, S et al. [15] provides the DL-based classifier to defend against the DDoS attack. Users' service requests are gathered as well as categorized as log information. To shorten the classifier's training period, several crucial characteristics from the log file are selected for classification utilized the Bhattacharya distance measure. Elephant Herd Optimization (EHO) is modified with the Taylor series in this case to create a Taylor-Elephant Herd Optimization-rooted Deep Belief Network (TEHO-DBN), and the algorithm created as a result is used to train the Deep Belief Network (DBN) for the detection of DDoS attacks.

Ogini et al. [16] The resource-constrained IoT devices employed in IoT are now relaxed for an attacker to crack due to the numerous weak IoT devices with high computing power. In order to recognise and stop DDoS attacks in the IoT computer environment, this research proposed an ensemble ML model utilizing the bagging approach. In a ML experiment, the model used data from the most recent DDoS attacks (CICDoS 2019).

2.3 Spoofing attack Security in IoT-Based Cloud Computing

Zaguia et al. [17] described security authorizations, encrypted communication routes, as well as device authentication, the integrity along with confidentiality of medical data. The proposed scheme's communication environment, as well as the trust boundary, along with the communication devices, such as the "starting" and "authentication" processes are also described. Additionally, the proposed communication protocols are described in

depth, also the symbols along with abbreviations that are used throughout the study are fully shown. Communicating a body sensor network (BSN) server to register, creating a secret key, along with allocating a track sequence number are all part of the startup procedure. The local processing unit (LPU), the BSN server, and the biosensors all need to be in secure contact for the proposed systematic verification to work.

Gayathri, et al. [18] described a method for preventing DDoS and fake data injection attacks is proposed in order to confirm the IoT devices security in the cloud. The proposed remedy is grounded on the integration of the access control lists (ACL), the Kullback-Leibler distance (KLD), along with the moving target defence (MTD) methods. The ACL as well as MTD strategies are used to combat these attacks by toughening the target in addition lowering the attack surface. The SNMP along with KLD methods are utilized to notice DDoS along with fraudulent data sharing attempts.

Khan et al. [19] discusses security and privacy issues as hybrid devices are used by more major organisations. The majority of the security techniques along with protocols offered by researchers are based on accepted Internet security norms. As a fundamental security need for protection against unauthorised access, the utmost suitable as well as widespread authentication feature for all sorts of IoT-based devices was among the top-ranking authentication feature categories. AI and ML may also be used to identify IoT device vulnerabilities and alert the relevant operator or administration for security.

Shafiq et al. [20] reviewed the most advanced IoT security solutions available today, with a focus on four key areas: (1) identifying potential solutions; (2) hand-selecting representative attacks; (3) acting a risk study along with result; along with (4) ranking keys as per the risks they mitigate. The research classified defence systems into five major categories by using this framework: DDoS detection along with prevention, default password protection, encryption techniques, anomaly detection as well as, intrusion detection and prevention. Regarding usefulness and usability, these solutions are still comparatively mature. However, only certain threats are considered in the security study, which may or may not be applicable to actual deployment. Threat modelling should be included in appropriate IoT security systems along with other considerations like resource usage and installation effort.

2.4 Port Scanning attack Security in IoT-Based Cloud Computing

Moubayed et al. [21] Along with some of the relevant material from the literature, a short overview of the security along with privacy issues and challenges that contemporary cloud-based networks are experiencing is offered. There is a description of the SDP idea, architecture, potential applications, and difficulties. An SDP-rooted framework with a client-gateway architecture is provided, and its result is assessed for a use case involving an internal corporate scenario on a virtualized network testbed. The findings of the performance study demonstrate that, although requiring more time during initial connection establishment, the SDP-secured network is resistant to port scanning and DoS attacks.

Eskandari et al. [22] introduced Pass ban, a sophisticated intrusion detection system (IDS) capable of safeguarding linked IoT devices. The proposed result is that it can be installed straight on relatively inexpensive IoT gateways, fully using the brink computing paradigm to recognise cyberthreats as near to the relevant data sources as feasible. This work show that Passban can accurately and with very few false positives identify a variability of malicious traffic, HTTP also SSH brute force, SYN flood attacks as well as such as port scanning.

Rachit et al. [23] made a thorough analysis that identifies the hazards associated with the IoT system, security protocols, also measures offered in current years, with an emphasis on the forthcoming IoT security issues. This study provides a modernized evaluation of the IoT architecture and the standards also protocols suggested for the next generation of IoT systems. In accordance with IoT security needs, a comparison of the existing security models, standards, and protocols is given. Since doing so safeguards the hardware, software, and data from a variety of dangers and assaults, this research underlines the necessity for uniformity at the level of communication along with data audit. This study highlights the need for strategies that may be applied to various threat vectors.

Rashid et al. [24] gave method to protect against along with mitigate IoT cyber security risks in a smart city, we investigate an attack as well as anomaly discovery approach based on ML methods. For performance improvement of the detection system, the research also investigates ensemble approaches including bagging, boosting, and stacking, in contrast to other efforts that have concentrated on single classifiers. In addition, it also takes into account the cross-validation, feature selection, as well as classification of multi-classes for the subject matter under discussion.

2. 5. Botnet attack Security in IoT-Based Cloud Computing

Tzagkarakis et al. [25] suggested ConnSpoiler, a simple solution that quickly recognises the stream of algorithmically generated domains (AGDs) in order to identify IoT-based botnets. ConnSpoiler can operate well on IoT devices with limited system resources since it only requires a small number of resources to operate.

ConnSpoiler has a high likelihood (approximately 94%) of identifying infection before the compromised devices connect to C&C servers thanks to the use of a potent statistical method called threshold random walk (TRW), which may assist in stopping further attacks. ConnSpoiler also doesn't need additional work to classify harmful samples for the training phase since it just needs the benign domains to function.

Meidan et al. [26] forwarded the N-BaIoT approach, a cutting-edge network-rooted anomaly discovery technique for the IoT that takes network behaviour snapshots as well as uses deep auto encoders to find unusual network traffic coming from hacked IoT devices. To evaluate the methods, this study infected nine commercial IoT devices with BASHLITE and the well-known IoT-based botnet Mirai.

Hosseinpour et al. [27] introduced an artificial immune system (AIS)-based distributed and lightweight IDS. The cloud, fog, and edge layers are only a few of the three IoT structures in which the IDS is deployed. This study uses a smart data approach to analyse the intrusion alarms in the fog layer. It places the detectors in edge devices at the edge layer. In order to provide lightweight and effective intrusion detection, smart data is a highly promising strategy. It offers a way to identify quiet attacks like botnet attacks in IoT-based systems.

Snehi et al. [28] give a thorough examination of security results' vulnerabilities for software-defined cyber-physical systems. The article outlines the software-defined cyber-physical system's architectural components along with suggests using fog computing to address a variety of weaknesses. CC have been individually assessed for security vulnerabilities, with a attention on DDoS and IoT-based DDoS attacks.

2.6 Security algorithm in IoT-Based Cloud Computing

Sajid et al. [29] As the IoT links and enhances the decision support system of the whole network, this has several advantages right away but also poses a number of key challenges that necessity be solved to improve the everlasting consistency. In reality, resistance, the monitoring of load, and other securityhazards in the cloud state presents comparable challenges.

Refaee et al. [30] proposed a scalable and secure architecture for IoT-based healthcare data transfer grounded on an optimised routing protocol. The input medical data was first gathered via a variety of IoT devices, including sensors and wearable technology. Through the use of data cleaning and data reduction procedures, the raw data is pre-processed. Principal component analysis (PCA) and KNN imputation were used to lessen the dimensions of the data. The pre-processed data was used to extract the features applying modified local binary patterns (MLBP). The fuzzy dynamic trust-based RPL (FDT-RPL) protocol enhances the total data transmission security by integrating the FDT-RPL algorithm with the butter ant optimisation (BAO) method for low-power as well as lossy networks.

Patil et al. [31] gives the need for authenticity, anonymity, and security above accessibility, this effort combined encryption with access management. The article proposed a ML-based technique for safe cloud data storage. The Huffman algorithm, which reduces text data size along with storage, resource consumption, or transmission power, was first used to compress the data. In light of this, the compressed data is encrypted using a cutting-edge cryptographic method. The data is encrypted using this technique before being uploaded to the cloud. Then, by suggesting a Gaussian Kernel Radial Basis Function Neural Network optimised for the Weighted Chimp Algorithm, the malicious intent in the cloud platform is discovered. This malicious code poses a serious danger to individuals and businesses since it may propagate over cloud platform infrastructures. The proposed technique successfully locates harmful malware in the cloud. The proposed approach is contrasted with several approaches already in use, including Ciphertext Policy-Attribute Based Encryption (CP-ABE), Fully Homomorphic Encryption (FHE), as well as Quasi Modified Levy Flight Distribution Reversed Sheamir Algorithm (QMLFD-RSA).

Deepika et al. [32] employs an expanded zigzag image encryption technique with a higher tolerance for data attacks to classify diseases using image processing in a secure CC environment. For successful picture categorization, a fuzzy convolutional neural network (FCNN) technique was also given. With many layers of training, the decrypted pictures are utilized to classify the various stages of cancer. Following categorization, the findings were sent to the patients and clinicians who need them for further therapy.

Table 1: IoT Cloud Security Approaches Review

Ref.No	Methodology	Advantages	Limitations
Ahmed et al. [33]	The multi-cloud and Internet of Things (IoT) integration framework	Analyze the effectiveness of this assault in an IoT.	Cannot be used to manage malicious insiders.

Zhu et al. [34]	Short signature algorithm (ZSS signature), trusted third party (TPA)	CC is mostly used by the IoT to increase its compute and storage capacity.	It still has some security issues.
Kaur et al. [35]	DPTCM k-nearest neighbor method (DPTCM-KNN)	Accuracy, memory use, attack detection efficiency, processing, and network overheads are all improved.	It is less real-time effective.
Syed, Naeem Firdous [36]	Message Queuing Telemetry Transport (MQTT)	Refrain from using compromised IoT devices to conduct further cyberattacks.	It is important to consider battery use restrictions brought on by message delays, message loss, and message retransmissions.
Abdullayeva, Fargana J. [37]	Principal Component Analysis	High the efficiency of data clustering.	It has limitations with battery usage, message delays.
Hussain et al. [38]	IoT, Architecture, Security Policies, Privacy, Cyber Security challenges, along with countermeasures	Since the IoT may operate without human intervention, security issues are more difficult to solve.	Does not apply for real time.
Alkhamisi, Khalid [39]	Describe and examine the many security and privacy issues the IoT-based ecosystem faces.	This method is more secure, and productive.	Still this work has some security issues.
Aboti, Chiragkumar D [40]	Authentication mechanism to mitigate cyber risks.	Cyber security is achieved.	Since security is a top priority in it, this technology needs to be implemented with extra care.
Jadhav, Ravi, and Harshad Ithape [41]	Blockchain technologies	Works with IoT security	No real-time
Pothuganti, Swathi. [42]	Review of some arising technology	The use of CC technology has greatly improved, and it is now widely accepted in both public and private settings.	-
Nasir et al. [43]	BTC_SIGBDS (Blockchain-powered, Trustworthy, Collaborative, Signature-based Botnet Detection System)	Detects the intrusion	Still have some limitations with battery life, memory etc.
Kalidindi et al. [44]	Deep Stack Encoder Neural Network	As more sensors, devices, apps, databases, services, and people are connected, advancements result.	Future intensifications will alter the amount of input, output, and hidden layer neurons to further improve accuracy.
Ganapathy, Sannasi [45]	A Chinese Remainder Theorem (CRT).	Security threat in CC and the IoT areas is identified.	Has computational complexity.

Wang, Mingzhe, and Qiuliang Zhang [46]	The data access storage architecture is first optimized using HDFS, and the data access configuration of the information storage locations is then optimized using hash values.	The efficiency of file uploading and downloading, data processing, and fault tolerance rate are all significantly increased by the article. .	Has issues with data access storage.

3. Conclusion

In conclusion, the current study has shown the security difficulties associated with IoT and the integration of cloud infrastructure. The issues in this sector need the attention of many scholars and practitioners. To overcome some of the difficulties, new technologies, including certain computer technologies, will be included. However, there is a need to provide more effective and safe cryptographic solutions for the IoT's dynamic addressing field. In addition to standardization and periodic audits, the specific suggestion calls for the implementation of other good practices. As the number of IoT-enabled devices grows, it is crucial to handle the security issues that arise in order to guarantee data integrity along with confidentiality, in addition to system as well as data availability.

References

[1] Stergiou, Christos L., Elisavet Bompoli, and Konstantinos E. Psannis. "Security and Privacy Issues in IoT-Based Big Data Cloud Systems in a Digital Twin Scenario." *Applied Sciences* 13, no. 2 (2023): 758.

[2] Almolhis, Nawaf, Abdullah Mujawib Alashjaee, Salahaldeen Duraibi, Fahad Alqahtani, and Ahmed Nour Moussa. "The security issues in IoT-cloud: a review." In *2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA)*, pp. 191-196. IEEE, 2020.

[3] Kimani, Kenneth, Vitalice Oduol, and Kibet Langat. "Cyber security challenges for IoT-based smart grid networks." *International journal of critical infrastructure protection* 25 (2019): 36-49.

[4] Ahmad, Waqas, Aamir Rasool, Abdul Rehman Javed, Thar Baker, and Zunera Jalil. "Cyber security in IoT-based cloud computing: A comprehensive survey." *Electronics* 11, no. 1 (2021): 16.

[5] Ding, Li, Zhongsheng Wang, Xiaodong Wang, and Dong Wu. "Security information transmission algorithms for IoT based on cloud computing." *Computer Communications* 155 (2020): 32-39.

[6] Chaudhry, Shehzad Ashraf, Khalid Yahya, Fadi Al-Turjman, and Ming-Hour Yang. "A secure and reliable device access control scheme for IoT based sensor cloud systems." *IEEE Access* 8 (2020): 139244-139254.

[7] Naeem, Humaira. "Analysis of Network Security in IoT-based Cloud Computing Using Machine Learning." *International Journal for Electronic Crime Investigation* 7, no. 2 (2023).

[8] Chakraborty, Alakananda, Muskan Jindal, Mohammad R. Khosravi, Prabhishek Singh, Achyut Shankar, and Manoj Diwakar. "A secure IoT-based cloud platform selection using entropy distance approach and fuzzy set theory." *Wireless Communications and Mobile Computing* 2021 (2021): 1-11.

[9] Yu, Yicheng, Liang Hu, and Jianfeng Chu. "A secure authentication and key agreement schaeme for IoT-based cloud computing environment." *Symmetry* 12, no. 1 (2020): 150.

[10] Zhou, Lu, Xiong Li, Kuo-Hui Yeh, Chunhua Su, and Wayne Chiu. "Lightweight IoT-based authentication scheme in cloud computing circumstance." *Future generation computer systems* 91 (2019): 244-251.

[11] Wang, Feifei, Guosheng Xu, Guoai Xu, Yuejie Wang, and Junhao Peng. "A robust IoT-based three-factor authentication scheme for cloud computing resistant to session key exposure." *Wireless Communications and Mobile Computing* 2020 (2020): 1-15.

[12] Martínez-Peláez, Rafael, Homero Toral-Cruz, Jorge R. Parra-Michel, Vicente García, Luis J. Mena, Vanessa G. Félix, and Alberto Ochoa-Brust. "An enhanced lightweight IoT-based authentication scheme in cloud computing circumstances." *Sensors* 19, no. 9 (2019): 2098.

[13] Salim, Mikail Mohammed, Shailendra Rathore, and Jong Hyuk Park. "Distributed denial of service attacks and its defenses in IoT: a survey." *The Journal of Supercomputing* 76 (2020): 5320-5363.

[14] Syed, Naeem Firdous, Zubair Baig, Ahmed Ibrahim, and Craig Valli. "Denial of service attack detection through machine learning for the IoT." *Journal of Information and Telecommunication* 4, no. 4 (2020): 482-503.

[15] Velliangiri, S., P. Karthikeyan, and V. Vinoth Kumar. "Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks." *Journal of Experimental & Theoretical Artificial Intelligence* 33, no. 3 (2021): 405-424.

[16] Ogini, Nicholas Oluwole, Wilfred Adigwe, and Noah Oghenefego Ogwara. "Distributed Denial Of Service

Attack Detection And Prevention Model For Iot-Based Computing Environment Using Ensemble Machine Learning Approach." (2022).

[17] Zaguia, Atef. "Personal Healthcare Data Records Analysis and Monitoring using The Internet of Things and Cloud Computing." *Avicenna* 2023, no. 1 (2023): 4.

[18] Gayathri, Rajakumaran, Shola Usharani, Miroslav Mahdal, Rajasekharan Vezhavendhan, Rajiv Vincent, Murugesan Rajesh, and Muniyandy Elangovan. "Detection and Mitigation of IoT-Based Attacks Using SNMP and Moving Target Defense Techniques." *Sensors* 23, no. 3 (2023): 1708.

[19] Khan, Habib Ullah, Muhammad Sohail, Farhad Ali, Shah Nazir, Yazeed Yasin Ghadi, and Inam Ullah. "Prioritizing the multi-criterial features based on comparative approaches for enhancing security of IoT devices." *Physical Communication* 59 (2023): 102084.

[20] Shafiq, Muhammad, Zhaoquan Gu, Omar Cheikhrouhou, Wajdi Alhakami, and Habib Hamam. "The rise of "Internet of Things": review and open research issues related to detection and prevention of IoT-based security attacks." *Wireless Communications and Mobile Computing* 2022 (2022): 1-12.

[21] Moubayed, Abdallah, Ahmed Refaey, and Abdallah Shami. "Software-defined perimeter (sdp): State of the art secure solution for modern networks." *IEEE network* 33, no. 5 (2019): 226-233.

[22] Eskandari, Mojtaba, Zaffar Haider Janjua, Massimo Vecchio, and Fabio Antonelli. "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices." *IEEE Internet of Things Journal* 7, no. 8 (2020): 6882-6897.

[23] Rachit, Shobha Bhatt, and Prakash Rao Ragiri. "Security trends in Internet of Things: A survey." *SN Applied Sciences* 3 (2021): 1-14.

[24] Rashid, Md Mamunur, Joarder Kamruzzaman, Mohammad Mehedi Hassan, Tasadduq Imam, and Steven Gordon. "Cyberattacks detection in iot-based smart city applications using machine learning techniques." *International Journal of environmental research and public health* 17, no. 24 (2020): 9347.

[25] Tzagkarakis, Christos, Nikolaos Petroulakis, and Sotiris Ioannidis. "Botnet attack detection at the IoT edge based on sparse representation." In *2019 Global IoT Summit (GIoTS)*, pp. 1-6. IEEE, 2019.

[26] Meidan, Yair, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher, and Yuval Elovici. "N-baiot—network-based detection of iot botnet attacks using deep autoencoders." *IEEE Pervasive Computing* 17, no. 3 (2018): 12-22.

[27] Hosseinpour, Farhoud, Payam Vahdani Amoli, Juha Plosila, Timo Hämäläinen, and Hannu Tenhunen. "An intrusion detection system for fog computing and IoT based logistic systems using a smart data approach." *International Journal of Digital Content Technology and its Applications* 10, no. 5 (2016).

[28] Snehi, Manish, and Abhinav Bhandari. "Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks." *Computer Science Review* 40 (2021): 100371.

[29] Sajid, Faiqa, Muhammad Abul Hassan, Ayaz Ali Khan, Muhammad Rizwan, Natalia Kryvinska, Karovič Vincent, and Inam Ullah Khan. "Secure and efficient data storage operations by using intelligent classification technique and RSA algorithm in IoT-based cloud computing." *Scientific Programming* 2022 (2022): 1-10.

[30] Refaee, Eshrag, Shabana Parveen, Khan Mohamed Jarina Begum, Fatima Parveen, M. Chithik Raja, Shashi Kant Gupta, and Santhosh Krishnan. "Secure and scalable healthcare data transmission in IoT based on optimized routing protocols for mobile computing applications." *Wireless Communications and Mobile Computing* 2022 (2022): 1-12.

[31] Patil, Rupali S., Amina Kotwal, And Swati S. Patil. "Efficient Iot-Based Cloud Computing Framework For Secure Data Storage Using Machine Learning Algorithm." *Journal Of Theoretical And Applied Information Technology* 101, No. 10 (2023).

[32] Deepika, J., C. Rajan, and T. Senthil. "Security and privacy of cloud-and IoT-based medical image diagnosis using fuzzy convolutional neural network." *Computational Intelligence and Neuroscience* 2021 (2021): 1-17.

[33] Ahmed, Afsheen, Rabia Latif, Seemab Latif, Haider Abbas, and Farrukh Aslam Khan. "Malicious insiders attack in IoT based multi-cloud e-healthcare environment: a systematic literature review." *Multimedia Tools and Applications* 77 (2018): 21947-21965.

[34] Zhu, Hongliang, Ying Yuan, Yuling Chen, Yaxing Zha, Wanying Xi, Bin Jia, and Yang Xin. "A secure and efficient data integrity verification scheme for cloud-IoT based on short signature." *IEEE Access* 7 (2019): 90036-90044.

[35] Kaur, Gaganjot, and Prinima Gupta. "Detection of distributed denial of service attacks for IoT-based healthcare systems." *Computer Assisted Methods in Engineering and Science* 30, no. 2 (2022): 167-186.

[36] Syed, Naeem Firdous. "IoT-MQTT based denial of service attack modelling and detection." (2020).

[37] Abdullayeva, Fargana J. "Distributed denial of service attack detection in E-government cloud via data clustering." *Array* 15 (2022): 100229.

[38] Hussain, Altaf, Amir Hussain, Shah Marjan, Mehmood Baryalai, Zubair Zaland, Abdul Wahid, and Shumaila Hussain. "Cyber Security Challenges and Attacks and Countermeasures for IoT-Based Smart Home." *Journal of Applied and Emerging Sciences* 12, no. 2 (2022): 166-172.

[39] Alkhamisi, Khalid. "An Analysis of Security Attacks on IoT Applications." *International Journal of Information Systems and Computer Technologies* 2, no. 1 (2023).

[40] Aboti, Chiragkumar D. "Studies of Challenges to Mitigating Cyber Risks in IoT-Based Commercial Aviation." *International Journal for Scientific Research and Development* 7 (2020): 133-139.

[41] Jadhav, Ravi, and Harshad Ithape. "Security Challenges observed in IoT-Enabled Cloud Infrastructure: A Review."

[42] Pothuganti, Swathi. "Overview on security issues in cloud computing." (2020).

[43] Nasir, Muhammad Hassan, Junaid Arshad, and Muhammad Mubashir Khan. "Collaborative device-level botnet detection for internet of things." *Computers & Security* 129 (2023): 103172.

[44] Kalidindi, Archana, and Mahesh Babu Arrama. "Enhancing IoT Security with Deep Stack Encoder using Various Optimizers for Botnet Attack Prediction." *International Journal of Advanced Computer Science and Applications* 14, no. 6 (2023).

[45] Ganapathy, Sannasi. "A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications." *Computer Networks* 151 (2019): 181-190.

[46] Wang, Mingzhe, and Qiuliang Zhang. "Optimized data storage algorithm of IoT based on cloud computing in distributed system." *Computer Communications* 157 (2020): 124-131.

Authors Contributions

Dr.Awatef Salem Balobaid[1]: Conceptualization, Investigation

Sameena Shaik[2]: Visualization, Writing original draft preparation

Sangeetha Komandur :Writing, reviewing and editing.

Conflicts of Interest

The authors declare no conflicts of interest