International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN(Online): 2347-5552, Volume-12, Issue-2, March 2024
https://doi.org/10.55524/ijircst.2024.12.2.5
Article ID IJIRD-1271, Pages 32-38
www.ijircst.org

Cyber Attack Detection Using Machine Learning Techniques in IoT Networks

Mansoor Farooq[1], and Mubashir Hassan Khan[2]

[1] Assistant Professor IT, Department of Management Studies, University of Kashmir, Kashmir, India
[2] Assistant Professor, Department of Computer Science, Cluster University of Srinagar, Kashmir, India

Correspondence should be addressed to Mansoor Farooq; mansoor.msct@uok.edu.in

Received 21 February 2024; Revised 4 March 2024; Accepted 15 March 2024

ABSTRACT- The Internet of Things is a rapidly emerging technology (IoT). Thanks to numerous sensors, billions of smart objects (referred to as "Things") may acquire data about themselves and their environment. So they may regulate and monitor industrial services or increase commercial services and activities. However, the Internet of Things is now more vulnerable than ever. Machine Learning (ML) has advanced significantly, bringing up new research avenues to solve current and future IoT challenges. On the other hand, machine learning is an effective method for identifying peril in intelligent devices and networks. Following a thorough literature review on Machine Learning methods and the necessity of IoT security, this study will assess numerous ML algorithms for threat detection and the various security methods which are associated with Machine Learning techniques.

KEYWORDS- Internet of Things (IoT), Machine Learning and IoT Attacks

I. INTRODUCTION

IoT links electrical equipment to a server and distributes data without the need for human intervention [1-4] [5,6]. Users may operate computers remotely from any location, rendering them open to a variety of attacks. As a consequence, the rising number of intelligent devices today raises security concerns for the IoT system, as the devices store private and important user information [1,4,6]. Kevin Ashton coined the phrase "internet of things" in a 1999 research presentation. IoT has been used in a variety of connection protocols to establish a link between people and the virtual world through smart devices and associated services. [7,8]. Smart home and portable devices, for example, give information on the buyer's position, contact information, health information, and so on, all of which must be kept secure and secret [9]. Because most IoT devices are resource restricted (i.e., batteries, bandwidth, storage, and computation), highly flexible and advanced algorithm-based security solutions are not accessible [10-12].Many IoT and machine learning methods, including deep learning and classifiers, have been implemented in intrusion detection systems, image analysis systems, and recommendation systems [13,14].Machine learning (ML) methods are a great way to keep IoT projects reliable. ML is a cutting-edge artificial intelligence technology that isn't difficult and can outperform complex networks [11] [15]. A vast variety of assaults as well as a To teach a machine, ML approaches are used to design a safety strategy. Furthermore, advances in Machine Learning look promising in terms of recognising and intelligently treating new threats through learning abilities. Future IoT device security standards will also improve the reliability and accessibility of machine learning algorithms [16,17].Below is the overall blueprint of this article: A general overview of the Internet of Things (IoT) and its security is provided in Section 2, which includes levels as well as the importance of IoT security. Section 3 discusses IoT assaults, their effect, and numerous attack surfaces, machine learning in IoT security, which includes several kinds of learning algorithms and IoT security solutions. Section 4 gives an overview of machine learning-based IoT security, while Section 5 gives an overview and discussion that were evaluated. Finally, Section 6 summarises the survey's findings.

II. INTERNET OF THINGS (IOT) LAYERS AND SECURITY

It is known as "the Internet of Things" (IoT) because it refers to the network of physical items, or "things," that are implanted with sensors, software, or other technologies to communicate and exchange data over the internet. Many of these gadgets may be found in the home, as well as in the workplace. Anything from a pill to an aeroplane may now be turned into a component of the IoT [19-22] thanks to the development of low-cost computer processors and a broad-based wireless network. Artificial intelligence may be applied to otherwise dumb equipment by connecting and adding sensors to them, without the need for a human, they can send real-time data. It is via the Internet of Things (IoT) that our society will become more intelligent and flexible [18, 23-25]. The IoT architecture is a gateway to multiple hardware applications to make a link and enhance IoT's services at each entryway [26]. To send and receive information/data from different levels of the IoT architecture, several networking protocols such as Bluetooth, Wi-Fi, RFID, narrow and broadband, ZigBee, and LPWAN are used [23,27].Physical, network, and application layers make up the majority of an IoT architecture [28,29].

A. Physical Layer

This layer is characterised by sensing and knowledge gathering and collection about the environment in which intelligent things are accessible [1,4,6] as shown in Figure 1.

Figure 1: Physical Layer devices in IoT

B. Network Layer

It is possible to transfer and process information utilising the internet connection provided by the various devices [1, 4, 6] because of the layer capability shown in Figure 2.

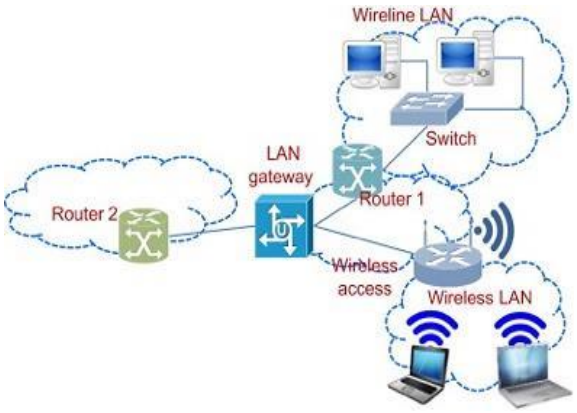

Figure 2: Network Layer devices in IoT

C. Application Layer

Its most important job is to give the user a specific application-based service that they have requested. [1,4,6] shown in Figure 3.

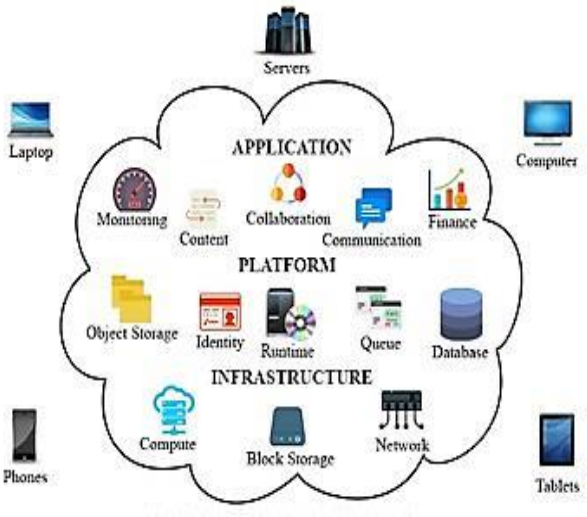

Figure 3: Application Layer devices in IoT

In the twenty-first century, IoT device security has been a hot topic. On one hand, IoT connects and brings the whole world closer together. On the other hand, it creates several entry points for diverse types of assaults [30-32].IoT applications are utilised for a variety of functions via an open network, making devices more user-friendly [33]. Due to countless dangers and attacks, the Internet of Things puts human life at risk, but it also makes it simpler and more obedient in technical terms. [34,35]. Because individual IoT devices may be viewed from anywhere without user authorization, IoT device security is becoming a major problem [35,36]. A broad range of security technologies must be applied to safeguard IoT goods. However, the physical construction of IoT devices restricts their computer capabilities, making it difficult to build a comprehensive security protocol [37,38] shown in Figure 4 and IoT device estimation is shown in Figure 5.

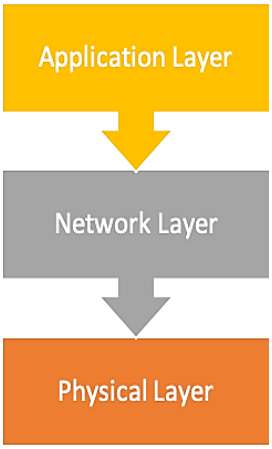

Figure 4: IoT Layer Architecture

When establishing a stable IoT, it's critical to think about the criteria that define protection. Security standards in a conventional IoT application are divided into three categories: (I) secrecy, (ii) integrity, and (iii) authentication [39].

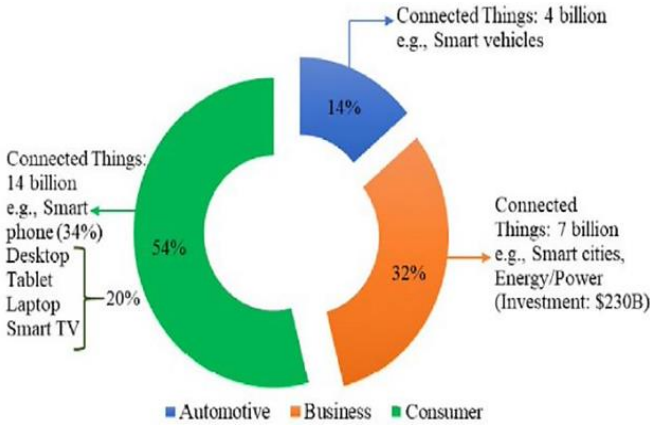

Figure 5: IoT Device User Estimation by 2024

- Confidentiality refers to keeping information hidden from other parties. Sensitive sensors, for example, need concealment when dealing with sensitive military information. One of the most often requested features is the Wireless Sensor Network (WSN) technology. Forces may be misled if a WSN's reports can be falsified, which may favour the opponent. Confidentiality is equally

important in essential social and industrial applications [39].

- To maintain the integrity of IoT data, the communication receiver must guarantee that messages received during transmission or delivery have not altered. The data integrity ensures that the information supplied is neither tampered with or corrupted. It is especially important because, even if attackers are unable to access data, the network may not function properly if compromised nodes corrupt the data provided. Indeed, if the communication link is unreliable, data may be altered without the intervention of an intruder. Integrity control ensures that both unintentional and intentional message modifications are recognised [39].
- The authentication procedure verifies whether a transmission originates from the intended recipient.It is asserted or declared to be what it is. The sensor nodes are responsible for determining the identity and validity of the peer node they are communicating with. Authenticity guarantees that the message is genuine. The Communication Authentication Code (MAC) is a piece of information that is used to verify the integrity and authenticity of a message [39,40].

III. IOT ATTACKS AND THEIR EFFECTS

There have been a number of assaults on the Internet of Things (IoT) system over the last several years, which has made both IoT manufacturers and customers more vigilant. Attacks, impacts and IoT surfaces are all covered in this section. Cyber and physical attacks are the two main forms of IoT attacks. As seen in Figure 6, cyberattacks may be either passive or aggressive. The user's data may be stolen, erased, changed, or destroyed on a wireless network by a cyber-attack threat that targets many IoT devices. Assaults by humans, on the other hand, may lead IoT devices to suffer physical injury.Attacking a device in this manner does not need a network connection. The physical IoT devices mentioned above are likewise vulnerable to similar attacks [30 43]. The following subsections focus mostly on the numerous cyberattack forms as two primaries cyberattack kinds [30].

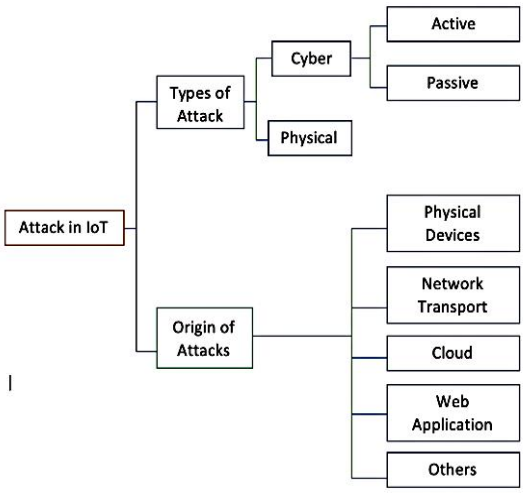

Figure 6: IoT attacks and their origin

A. Active IoT Attacks

Any time a hacker gains control of a computer network and disables essential services, this is considered an active assault. Interruptions, interventions, and changes in ongoing assaults are just a few of the methods attackers might use to compromise IoT device security.

- **Denial-of-Service (DoS) assaults**, as seen, are system service disruptions that are the most prevalent cause of system outages. Or to put it another way, the IoT device does not allow the user to make informed choices. DoS attacks reduce the battery life of IoT devices because of their continual use[46-48]. "Distributed denial of service" attacks aim to overload servers by flooding them with requests (DDoS). This makes it impossible to discriminate between legitimate and malicious communications [46,47]. DDoS attacks launched by a Mirai IoT botnet infection have resulted in thousands of IoT devices failing as a consequence of interference [30,41].
- **Spoofing and Sybil attacks**: these sorts of assaults are mostly employed to obtain unauthorised access to IoT systems, IoT devices are especially susceptible to spoofing attacks because TCP/IP lacks a comprehensive security protocol. Man-in-the-middle assaults and denial of service are both started by these two attacks, as well [30][21].
- **They were jamming attacks**: Constant wireless network connectivity through the transmission of unwanted signals to IoTT devices causes problems for users by keeping the network always busy, as illustrated. Adding insult to injury, this sort of attack consumes more memory, bandwidth, and other resources in IoT systems [30].
- **Man-in-the-middle attacks:** are carried out by network users who are directly connected to another user interface, As a consequence, adding false or inaccurate data to the original data is an easy way to interrupt communications [30,33,44].
- **Selective Forwarding attacks**: If the transmission attack operates as a node of the communication device, it may be dropped to create a networking hole, while transmitting, as shown in the illustration above. This kind of assault is difficult to identify and stop [30].
- **Malicious Input attacks**: An example of harmful input assaults [30], which includes attacks by malware, such as Trojan horses (also known as rootkits), rootkit-enabled worms, and adware.
- **Hole Attacks:** attacks such as Blackhole and Grayhole degrade network performance and may cause the network to crash.
- **Data Tampering:** Data tampering is a serious hazard to everyone's life and possessions, not just businesses. Because of this, firms must take steps to prevent and minimise the harm caused by such attacks, as shown in Figure 6 [30].

B. Passive IoT Attacks

Passive attacks are intended to gather personal information about the user and decode their encrypted data without the user's awareness [15,16]. Passive attacks on IoT networks often include eavesdropping and traffic monitoring [27].

- **Eavesdropping**: In eavesdropping, the attacker eavesdrops on communications between two people. For

the attack to work, the traffic must not be encrypted. For example, a password submitted in response to an HTTP request may be obtained unencrypted [47,48].

- **Traffic analysis:** To get information about traffic exchanged and the parties involved, an attacker analyses the metadata that is sent in traffic (rate, duration, etc.). Cryptanalysis attacks can occur if encrypted data is used in traffic analysis, resulting in unencrypted information or successful traffic.

The effect of IoT attacks on the network is a danger to the privacy, authentication, and consent of users. All of the numerous assaults, as well as their impact on IoT devices, are shown in Figure 7. The following elements must be addressed while creating a security protocol for IoT device attacks [30,39].

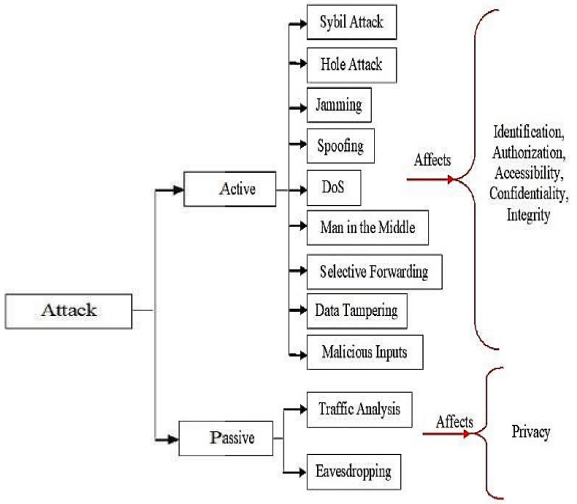

Figure 7: Active and passive attacks with their effects [30].

IV. MACHINE LEARNING (ML) APPLICATIONS IN IOT ATTACK DETECTION

To teach machines, ML employs diverse methods and lets robots learn from their encounters rather than being explicitly programmed [16]. ML does not need the participation of humans, sophisticated mathematical techniques, or the use of large networks [25,26]. Recent advances in machine learning (ML) for IoT security have been significant. ML methods may therefore predict distinct IoT assaults based on an early assessment of system behaviour. In addition, merging different ML algorithms may give appropriate solutions for resource-limited IoT devices. ML Techniques and ML-based IoT Security Technologies are the two subsections of this section [16].

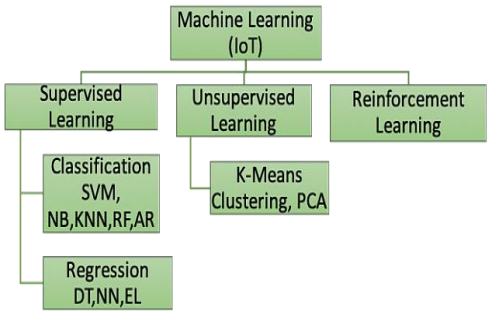

Figure 8: Machine Learning Model

A. Machine Learning (ML) Techniques

To teach machines, ML employs diverse methods and lets robots learn from their encounters rather than being explicitly programmed [16]. ML does not need humanitarian aid, sophisticated math methods, or complex network performance [35,36]. In recent years, ML techniques for IoT security have evolved significantly. Thus, ML methods may predict distinct IoT threats by studying system behaviour early on. In addition, merging different ML algorithms may give appropriate solutions for resource-limited IoT devices. There are two subcategories in this section: IoT Security Using Machine Learning and Machine Learning-based Techniques [16]. IoT devices may be protected using ML approaches such as supervised techniques, unsupervised techniques, and reinforcement learning. For IoT device security, Figure 8 displays a variety of machine-learning techniques.When it comes to machine learning, the most prevalent technique is supervised learning, in which an algorithm is used to evaluate the output according to the input. Classification and regression are two types of supervised learning. There is no output data for these input variables in Unsupervised Learning. The system tries to find connections between the data it collects, which is why the majority of it is left unlabelled. Various classes are grouped in these clusters [37]. It is also possible for machines to learn in the same manner that people do, by acting in a way that maximises total feedback. Depending on how the mission goes, the feedback may be a kind of compensation. Reinforcement learning relies on trial and error rather than predetermined behaviours for each activity. Trial and error may be used by the agent to discover and implement the optimum method for the biggest reward [30].

B. Machine Learning-Based Solution for IoT Attack Detection

It has arisen as a new study subject in the past few years, capturing the attention of today's scholars who want to add more to it. To keep IoT devices safe, many ML methods have been presented in this area. The physical/perception layer, the network layer, and the web/application layer of an IoT structure were used in the development of these solutions [30].The exact threshold value for detecting undesired transmissions that create false alarms makes traditional authentication systems for securing the physical surface inadequate. As a consequence, methods based on machine learning might be utilised to authenticate at the physical layer [30]. Zhuo and Liu, 2016 [39] Authentication errors were reduced by 64.3% using QL-based learning approaches, which outperformed the industry benchmark of 12 stages of authentication. For supervised ML approaches such as Distributed Frank Wolf and Incremental Aggregated Gradient, further research has been done to create parameters for the logistical regression model to minimise the communication cost and boost spoofing detection performance Recently, Kiran, 2018 [41] came out with an all-encompassing ML-based technique for protecting IoT PCs. In essence, it lets authorised users to access to the system and safely archive the data of other allowed users.. of users.. Peer-to-peer encryption protocols in the IoT architecture would need clients to register with the cloud registry beforehand.Neural and ElGamal algorithms paradigms were proposed by Alam et al., 2018 [36] for the prevention of assaults and the stability of IoT

devices. In this case, private and public keys were used to control the cryptosystem. After categorising the data, it is compared to the training data. There is also the novel security approach of Baracaldo and colleagues to detect and filter harmful data acquired to create an unsupervised mode [24]. Even if the assault is common, network security is a problem that links the actual world with the virtual one. The intruder assault may thus be detected by several machine learning techniques such as SVM, NN, and KNN 2016 [29] by Saied et al. A DDoS attack detection model was proposed using an ANN algorithm. Network traffic will be restricted to just authentic data packets under the proposed approach. When trained on changed data sets, the ANN was able to identify DDoS assaults better than before.

C. Challenges and Gaps

It's hard to escape the influence of the Internet of Things these days. IoT security has also grabbed the curiosity of many network and device experts, who are eager to learn more about it. Because of the many issues raised by IoT's deployment, usage, and impact on networks, new research directions are likely to come up [45]. The use of machine learning (ML) is a feasible alternative to traditional IoT frameworks. Innovative artificial intelligence technology ML doesn't need explicit programming and may be achieved in complicated networks [30] The root causes of security and privacy issues must be identified and addressed before IoT can be effectively used. Current technology has thrown about the idea of the Internet of Things (IoT), so the safety concerns are still new. Existing technology should be improved upon [22]. IoT and IT security issues were examined by Fernandes et al., 2017 [86] in their study. They have concentrated on privacy issues. Software, electronics, networks, and applications have a major role in determining the similarities and differences across products. IoT security issues are largely the same as those in traditional IT, according to this categorization. IoT's biggest worry, however, is the lack of resources available to alter the advanced security solutions in IoT networks. Additionally, IoT security and privacy solutions cross-layer protection requires a cross-cutting layer design and optimised algorithms. Due to computational limits, IoT systems may need new breeds of efficient cryptography and privacy algorithms. However, as the number of IoT devices grows, more issues with security standards will inevitably arise. The most difficult defences don't rely on one-off fixes. In the case of a DDoS or incursion assault, for example, false-positive findings may render the remedies worthless. In addition, the market's faith in these solutions would be eroded, and their efficiency would decline. IoT security and privacy may benefit from a systematic strategy that incorporates existing safety technologies and creates intelligent, scalable security solutions for the IoT [11].

V. ASSESSMENT AND RECOMMENDATIONS

Researchers employed a variety of ML algorithms and strategies to identify attacks and anomalies, as shown in Table 1, and they achieved impressive detection accuracy results. It has been shown that the Random Forest (RF) algorithm performs the best in studies [23][32][43][45], [40] when compared to other ML algorithms utilised and compared by researchers [41][42][43][44][45]. I was at school at the time. This study's findings demonstrate that, when compared to DT, KNN performs better. However, KNN takes more time to categorise than does DT.

Table 1: Comparison of ML algorithms for attack detection in IoT networks with performance

Author	Objectives	Technique	Datasets	Result and Accuracy
Alsamiri et al. [47]	Detecting IoT attacks quickly	Naïve Bayes, RF, ID3, Adaboost, MLP, QDA and KNN	Bot-IoT	The accuracy for the used ML algorithms was Naïve Bayes was 0.77; the Random Forest was 0.98, ID3 was 0.98; Adaboost had 0.98, MLP was 0.84, QDA was 0.86, and KNN was 0.99.
Stoian [22]	Anomaly Detections and Attacks in IoT Networks.	RF, NB, MLP, SVM, and AdaBoost.	IoT-23	The RF algorithm has obtained the best results with 99.5% accuracy
Hasan et al., [46]	Many machine learning models have been tested for their ability to anticipate IoT network threats and abnormalities.	LR, DT, RF, SVM, and ANN.	NSL-KDD, Real Traffic, DS2OS	Random Forest has recorded the best accuracy 99.4 %
Susilo and Sari [44]	Improving IoT Security by using machine learning techniques	Random Forest, CNN, and MLP	BoT-IoT	Random forests and CNN have recorded the highest results in terms of accuracy
Rani and Kaushal, [45]	Improve the security and accuracy of Intrusion Detection System (IDS)	KNN, NB, Decision Tree, Logistics Regression, RF	NSL-KDD and KDDCUP99	The proposed simulation has a 99.9 per cent accuracy with less time and energy.

RF and DT, two machine learning methods, were combined in research [46] to improve the detection of attacks. When it comes to identifying assaults, the two machine learning algorithms, RF and KNN, were shown to be 99 percent accurate in investigations [47]. According to the research analysed, the Random Forest ML method performs best in terms of identifying attacks and anomalies.To cope with a variety of IoT-specific difficulties, machine learning (ML) has shown its utility in general cybersecurity applications. A broad range of IoT network vulnerabilities may be balanced by ML-based solutions because of their speed and adaptability. Research in machine learning (ML) for a wide range of applications is thriving. As an emerging technology, machine learning has a lot of data to back it up.

VI. CONCLUSION

In the future, the Internet of Things will allow us to access global themes and revolutionise the world. As a result, IoT smart services users will be able to exchange data with one other and keep it almost everywhere they have internet access. The security of IoT devices is a worry, even though they link us to the virtual world and make our lives easier, faster, and simpler. Based on a comprehensive review of the literature, this article takes an in-depth look at a wide range of security threats, algorithms, and solutions for the Internet of Things using machine learning (ML) (IoT). This paper's focus on embedded Machine Learning algorithms provides an overview of a wide range of IoT perils and their implications. Machine Learning algorithms have also been studied by academics to help future researchers outline their ultimate goals and objectives.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] Khan MA, Salah K. "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems. 2018;82:395-411.

[2] Farooq M. Supervised learning techniques for intrusion detection system based on multi-layer classification approach. International Journal of Advanced Computer Science and Applications. 2022;13(3).

[3] Lu Y, Da Xu L. "Internet of Things (IoT) cybersecurity research: A review of current research topics," IEEE Internet of Things Journal. 2018;6:2103-2115.

[4] Singh RP, Javaid M, Haleem A, Suman R. "Internet of things (IoT) applications to fight against COVID-19 pandemic," Diabetes & Metabolic Syndrome: Clinical Research and Reviews. 2020;14:521-524.

[5] Farooq M, Hassan M. IoT smart homes security challenges and solution. International Journal of Security and Networks. 2021;16(4):235-43.

[6] Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. "A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues," IEEE Communications Surveys & Tutorials. 2020;22:1191-1221.

[7] 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. 2019;7:82721-82743.

[8] Farooq M. Genetic algorithm technique in hybrid intelligent systems for pattern recognition. International Journal of Innovative Research in Science, Engineering and Technology. 2015;4(04):1891-8.

[9] Adat V, Gupta B. "Security in Internet of Things: Issues, challenges, taxonomy and architecture," Telecommunication Systems. 2018;67:423-441.

[10] Fawzi LM, Alqarawi SM, Ameen SY, Dawood SA. "Two Levels Alert Verification Technique for Smart Oil Pipeline Surveillance System (SOPSS)," International Journal of Computing and Digital Systems. 2019;8:115-124.

[11] Al-Sultan MR, Ameen SY, Abduallah WM. "Real Time Implementation of Stegofirewall System," International Journal of Computing and Digital Systems. 2019;8:498-504.

[12] Farooq M, Khan MH. Artificial Intelligence-Based Approach on Cybersecurity Challenges and Opportunities in The Internet of Things & Edge Computing Devices. International Journal of Engineering and Computer Science. 2023 Jul;12(07):25763-8.

[13] Ammar M, Russello G, Crispo B. "Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications. 2018;38:8- 27.

[14] Chernyshev M, Baig Z, Bello O, Zeadally S. "Internet of things (iot): Research, simulators, and testbeds," IEEE Internet of Things Journal. 2017;5:1637-1647.

[15] Farooq M, Khan MH. Signature-Based Intrusion Detection System in Wireless 6G IoT Networks. Journal on Internet of Things. 2022 Jul 1;4(3).

[16] Vashi S, Ram J, Modi J, Verma S, Prakash C. "Internet of Things (IoT): A vision, architectural elements, and security issues," in 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). 2017;492-496.

[17] Sharma B, Sharma L, Lal C. "Anomaly Detection Techniques using Deep Learning in IoT: A Survey," in 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE). 2019;146-149. Janaby AO. al, A. Al-Omary, S. Y. Ameen, and H. M. Al-Rizzo, "Tracking High-Speed Users Using SNR-CQI Mapping in LTE-A Networks," in 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT). 2018;1-7.

[18] Farooq M. Application of genetic algorithm & morphological operations for image segmentation. International Journal of Advanced Research in Computer and Communication Engineering. 2015 Mar;4(3):195-9.

[19] Costa KA. da, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," Computer Networks. 2019;151:147-157.

[20] Hussain F, Hussain R, Hassan SA, Hossain E. "Machine learning in IoT security: Current solutions and future challenges," IEEE Communications Surveys & Tutorials. 2020;22:1686- 1721,

[21] Farooq M, Khan R, Khan MH. Stout Implementation of Firewall and Network Segmentation for Securing IoT Devices. Indian Journal of Science and Technology. 2023 Sep;16(33):2609-21.

[22] Othman A, Ameen SY, Al-Rizzo H. "Dynamic Switching of Scheduling Algorithm for," International Journal of Computing and Network Technology. 2018;6.

[23] Arko AR, Khan SH, A. Preety, M. H. Biswas, "Anomaly detection In IoT using machine learning algorithms," Brac University; 2019.

[24] Farooq M. Optimizing pattern recognition scheme using genetic algorithms in computer image processing. International Journal of Advanced Research in Computer Engineering & Technology. 2015 Mar;4(3):834-6.

[25] Hassan RJ, S. R. Zeebaree, S. Y. Ameen, S. F. Kak, M. A. Sadeeq, Z. S. Ageed, et al., "State of Art Survey for IoT Effects on Smart City Technology: Challenges, Opportunities, and Solutions," Asian Journal of Research in Computer Science. 2021;32-48.

[26] Ameen SY, Ali ALSH. "A Comparative Study for New Aspects to Quantum Key Distribution," Journal of Engineering and Sustainable Development. 2018;11:45- 57.
[27] Farooq M, Hassan M. Pattern recognition in digital images using fractals. International Journal of Engineering and Advanced Technology. 2019;9(2):3180-3.
[28] Malallah H, Zeebaree SR, R. R. Zebari, M. A. Sadeeq, Z. S. Ageed, I. M. Ibrahim, et al., "A Comprehensive Study of Kernel (Issues and Concepts) in Different Operating Systems," Asian Journal of Research in Computer Science. 2021;16- 31.
[29] Zebari IM, Zeebaree SR, Yasin HM. "Real Time Video Streaming From Multi-Source using Client-Server for Video Distribution," in 2019 4th Scientific International Conference Najaf (SICN). 2019;109-114.
[30] Farooq M. Color Edge Detection Based on the Fusion of Intensity and Chromatic Differences. International Journal of Recent Technology and Engineering (IJRTE). 2020;8(6):1038-41.
[31] Nižetić S, P. Šolić, D. L.-d.-I. González-de, and L. Patrono, "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future," Journal of Cleaner Production. 2020;274:122877.
[32] Khalid LF, S. Y. Ameen, "Secure Iot integration in daily lives: A review," Journal of Information Technology and Informatics. 2021;1:6-12.
[33] Farooq M. Enhancement and Segmentation of Digital Image using Genetic Algorithm. International Journal of Research in Electronics and Computer Engineering. 2019;7(2):2619-23.
[34] Alaba FA, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," Journal of Network and Computer Applications. 2017;88:10-28,
[35] Yasin HM, Zeebaree SR, M. A. Sadeeq, S. Y. Ameen, I. M. Ibrahim, R. R. Zebari, et al., "IoT and ICT based Smart Water Management, Monitoring and Controlling System: A Review," Asian Journal of Research in Computer Science. 2021;42- 56.
[36] Farooq M. Split/Merge and Chromosome Encoding Model of Genetic Algorithm For Image Segmentation & Optimization. International Journal of Advanced Research in Computer Science. 2015 Mar 1;6(2).
[37] Singh A, A. Payal, S. Bharti, "A walkthrough of the emerging IoT paradigm: Visualizing inside functionalities, key features, and open issues," Journal of Network and Computer Applications. 2019;143:111-151.
[38] Elazhary H. "Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions," Journal of Network and Computer Applications. 2019;128:105-140.
[39] Farooq M. Application of Genetic Programming for Pattern Recognition. International Journal of Advanced Research in Computer and Communication Engineering. 2015;4(4):14-7.
[40] Yasin HM, Zeebaree SR Zebari, IM. "Arduino Based Automatic Irrigation System: Monitoring and SMS Controlling," in 2019 4th Scientific International Conference Najaf (SICN). 2019;109-114.
[41] Tahsien SM, Karimipour H, Spachos P. "Machine learning based solutions for security of Internet of Things (IoT): A survey," Journal of Network and Computer Applications. 2020;161:102630.
[42] Novaliendry D, Farooq M, Sivakumar KK, Parida PK, Supriya BY. Medical Internet-of-Things Based Breast Cancer Diagnosis Using Hyper Parameter-Optimized Neural Networks. International Journal of Intelligent Systems and Applications in Engineering. 2024 Jan 7;12(10s):65-71.
[43] Gupta MK, Dwivedi RK, Sharma A, Farooq M. Performance Evaluation of Blockchain Platforms. In2023 International Conference on IoT, Communication and Automation Technology (ICICAT) 2023 Jun 23 (pp. 1-6). IEEE.
[44] Farooq M, Hassan M. "EDeLeaR: Edge-based Deep Learning with Resource Awareness for Efficient Model Training and Inference for IoT and Edge Devices", Int. J. Sc. Res. In Network Security and Communication. 2024; 12(1):1- 8.
[45] Gupta MK, Rai AK, Farooq M, Santhiya P. Network Security and Protection Strategies for Big Data: Challenges and Innovations. In2023 6th International Conference on Contemporary Computing and Informatics (IC3I) 2023 Sep 14 (Vol. 6, pp. 705-709). IEEE.
[46] Sharma A, Kumar G, Farooq M, Gupta MK, Raj S, Rai AK. Unleashing the Power of Big Data: A Comprehensive Analysis and Future Directions. In2023 6th International Conference on Contemporary Computing and Informatics (IC3I) 2023 Sep 14 (Vol. 6, pp. 828-832). IEEE.
[47] Farooq M, Khan MH. QuantIoT Novel Quantum Resistant Cryptographic Algorithm for Securing IoT Devices: Challenges and Solution.

ABOUT THE AUTHORS

Dr Mansoor Farooq (Member IEEE), an Assistant Professor at the University of Kashmir, brings a wealth of expertise in Network & Information Security, honed during his tenure as a Lecturer at the University of Technology and Applied Science, Al Musanna, Oman. With a background as a Computer Scientist specializing in AI, ML, and NLP, he earned his PhD from Shri Venkateshwara University, complemented by an MCA from the Islamic University of Science & Technology and a BCA from the University of Kashmir. A distinguished member of IEEE, ACM, and IAENG, Dr Farooq boasts a rich professional journey spanning 13 years, marked by a profound passion for Cybersecurity, AI, ML, and Cloud Computing & Security**.**

Mubashir Hassan Khan, an Assistant Professor at the Department of Higher Education, Ministry of Education, J&K, brings 15 years of experience to his role. With an MCA from the University of Kashmir, he has excelled as a Software Engineer at the same institution and led as Head of the IT Cluster University Srinagar. A dedicated member of ACM and IAENG, Khan's professional journey is fueled by his fervent interests in Cybersecurity, AI, ML, and Cloud Computing & Security**.**