The Open Biomedical Engineering Journal

Content list available at: https://openbiomedicalengineeringjournal.com

REVIEW ARTICLE

Strength of Deep Learning-based Solutions to Secure Healthcare IoT: A Critical Review

Arul Treesa Mathew[1] and Prasanna Mani[1,*]

[1] *School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu 632014, India*

Abstract:

Healthcare applications of IoT systems have gained huge popularity across the globe. From personal monitoring to expert clinical diagnosis, healthcare IoT systems have shown their importance to all possible extents. The ease of use and precise results add to the wide acceptance of such systems. However, this has also led to a magnificent increase in the number of attacks aimed at stealing or manipulating data as well as operations of HIoT-based healthcare assistance. Among the various modes of attacks, network-based attacks are found in the majority. In this work, we perform a critical review of these attacks, the existing countermeasures, and their limitations to understand and proclaim the importance of securing healthcare networks in the best possible manner. We also emphasize the necessity of deep learning-based smart solutions for securing healthcare systems, understanding the potential of deep learning in the security aspects being deployed in other genres of IoT applications. A comparative analysis of deep learning and machine learning-based security solutions is performed to examine their performances.

Keywords: Healthcare, Healthcare internet of things, Network attacks, Deep learning, IoT systems, Healthcare networks.

Article History	Received: August 24, 2022	Revised: January 30, 2023	Accepted: February 24, 2023

1. INTRODUCTION

Over the past decade, technology has grown exponentially, owing to the wide range of applications offered by Artificial Intelligence, the Internet of Things, *etc*. Healthcare sector has received a greater advantage in this aspect. The Internet of Things has taken over many procedures and also offers remote operations, which were earlier tedious and conducted on the premises of the medical practitioner. With the rapid and widespread acceptance of the Internet of Things in the healthcare sector (HIoT), the healthcare sector has taken a global phase shift.

Hegde *et al*. (2021) [1] performed an extensive survey on various smart monitoring systems offered to the healthcare sector using IoT. This article provides a basic idea of the operational behaviors of healthcare IoT systems. Healthcare IoT [2] based systems can be broadly classified into two subcategories, namely personal HIoT and clinical HIoT, based on their level of application. Personal HIoT mainly includes wearable devices, such as activity/heart-rate trackers, smart clothes, and smartwatches that are used for self-monitoring. These are meant to be adopted for regular monitoring and come without any expert-level guidance, except that is given along with the product. On the other hand, clinical HIoT devices are developed specifically for health monitoring and have to be used with the guidance and involvement of a medical practitioner, for example, glucose monitors, connected inhalers, *etc*. Clinical IoT systems are often set up in clinical environments. Clinical IoT systems which are used in home environments have to be regulated and approved for use only after clinical validation.

Healthcare IoT (HIoT) has helped to reduce the geographical limitations that restrict people from experiencing expert consultation significantly. It has also made regular check-ups remotely operable. The user-friendly nature of these assistive mechanisms offered by HIoT has added more to its widespread use and popularity. Such systems have great strength, especially during the pandemic times. Along with the widespread popularity and acceptance comes the increased risk of malicious attacks [3]. The sensitive nature of the contained information attracts attackers owing to the impact of a successful attack. The consequences of such an attack can even include the death of the patient. Hence, it is really important to safeguard the HIoT systems and their contained information.

Attacks on healthcare IoT systems [4] can be classified into various categories based on the nature of the attack, the surface of the attack, and the mode of attack. There are active attacks and passive attacks. The passive attack tries to steal the information without taking a chance to modify it, while active attacks try to alter the information or change the device

* Address correspondence to this author at the School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu 632014, India; E-mail: prasanna.m@vit.ac.in

DOI: 10.2174/18741207-v17-e230505-2022-HT28-4371-2, 2023, *17*, e187412072304060

configuration and other modifications to the system. There are internal and external attacks, where internal attacks are triggered by some internal participants of the system, and external attacks are launched from outside the system boundaries. There are physical attacks [5], datalink attacks, network attacks, transport attacks, and application attacks based on the area of attack. Attacks on healthcare IoT systems mainly include denial of service, man-in-the-middle attacks, replay attacks, jamming attacks, tampering attacks, Sybil attacks, synchronization attacks, *etc*. Many solutions have been proposed in order to tackle the attacks on healthcare IoT.

In this review, we perform a critical review of some of these solutions, focusing on works that address network-based attacks over healthcare IoT systems. We discuss various attacks against healthcare IoT systems, the privacy concerns in healthcare IoT, countermeasures suggested to tackle the attacks and the importance of deep learning applications in these aspects. The remaining part of the paper is organized as follows: section 2 summarises related literature with subsections that discuss the classification. Section 3 details the analysis and inferences, and section 4 concludes the work.

2. RELATED LITERATURE

Several papers related to our topic of discussion were reviewed. However, in this section, we summarize some important articles that had major contributions to our work. We have classified the summary into various subsections to provide a better understanding of the same.

2.1. Surveys on Security Challenges

Kolandaisamy *et al*. (2021) [6] discussed the security risks associated with IoT-based healthcare networks. They analyzed various attack modes, architectural differences, and various technologies that are designed to secure these systems. The architectural layers of the IoT environment were also explained, providing an insight into what and where the vulnerabilities are in each layer.

Sengupta *et al*. (2020) [7] performed a detailed survey on various attacks, security vulnerabilities, and viable block-chain based solutions that can be used to tackle these issues. The authors categorized and also performed a comparative analysis of earlier surveys in this area and consolidated various attacks on IoT networks and their variant characteristics.

Iqbal, *et al*. (2020) [8] reviewed the important threats, challenges, security requirements and viable countermeasures in the IoT generalized context. Threats like social engineering-based vulnerabilities, user unawareness, hardware vulnerabilities, denial of service attacks, their variants, *etc*., bring a huge risk to these IoT-based systems. Attacks on each layer of the IoT system were discussed in the article. Default security mechanisms might fail to address those trials, which include code modification, updated malware definitions, *etc*. They suggested software-defined security for better safety of IoT systems.

Challenges to IoT applications are mainly classified as hardware-based, software-based and network-based, as defined in a study conducted by Mohammad *et al*. (2019) [9]. Attacks on these systems are mainly aimed at either taking control of the system or stealing the contained information. The authors of the article also performed a case analysis on various types of attacks that target the different applications of IoT, like healthcare, smart cars, smart campus, smart farms, *etc*. Cilleruelo *et al*. (2021) [10] presented the security and privacy issues found across data-over-sound devices used in healthcare IoT systems. They suggested a reverse engineering-based method to analyze the security challenges in the system, thereby enabling suitable countermeasures. Ali and Mahmoud (2019) [11] mentioned various routing attacks found in healthcare IoT-based networks. Black hole attacks and delay attacks are explored in detail, and the authors also proposed a preventive mechanism that employs both presence and absence of AODV protocol. However, it could produce only a slight improvement in the system's performance.

Somasundaram and Thirugnanam (2021) [12] studied various security issues found in IoMT systems. They assessed the risks associated with IoMT-based systems by considering the probability and possible impact of the attacks. The possibility of an attack is related to the vulnerability levels of the medical device. The assessment revealed that DDoS-based attacks have higher impacts on IoMT-based systems. A. Ali and Mahmoud [13]. performed an analysis of the security strengths and challenges in IoT systems that operate in the healthcare environment. They adopted 2 protocols (SecRout and AODV) based on which the assessment was carried out. SecRout uses the symmetric cryptographic organization to ensure data. Its two-layer architecture helps in reducing communication overhead. AODV protocol offers better support for unicast and multicast routing schemes but is more prone to attacks. Table **1** shows the inferences from 2.1.

In this section, we consolidated various studies conducted to identify the security challenges and vulnerabilities in an IoT environment. The number of challenges identified is generic and could be applied to all the application domains of IoT. When the healthcare domain is specifically considered, these challenges send out an alert to safeguard the systems so that the sensitive data and devices are secured from malicious attacks.

Table 1. Inferences from 2.1.

References	Inferences	Gaps Identified
[1 - 13]	A better understanding of various security challenges to IoT systems and potential attack modes.	The articles discussed any one security challenge in detail and did not cover the chances of combinational exploits.

2.2. Attacks and Classifications

The authors (Rajendran *et al*. (2019)) [14] described various threats that are commonly found in IoT systems, classifying them based on the layer of attack, like IoT devices and peripherals, gateways and internal network elements, cloud and related elements. They also tabulated various countermeasures that could be employed to mitigate these threats. Sharma (2022) [15] put forward a solution to detect and prevent any jamming attacks that might be used against IoHT systems. The algorithm developed can analyze the strength of a signal received, the ratio of packet loss, and the number of devices disrupted, which might be the outcome of a jamming attack. This helps in enabling secure communication between IoHT devices and transferring confidential data without any hindrance.

Calvillo-Arbizu *et al*. (2021) [16] performed an in-depth analysis of the Internet of Things employed in the healthcare sector. They analyzed the scenario over three themes: the lifecycle of data, trust and privacy, and human-related issues. Qadri *et al*. (2020) [17] elaborated on the increasing popularity and widespread use of IoT systems in various areas, especially healthcare. They also discussed the limitations in the existing security mechanisms from the IoT perspective due to resource constraints. The main threats discussed were selective forwarding and wormhole routing-based attacks. The authors suggested a block-chain based solution to prevent the above-mentioned attacks.

Djenna and Eddine (2018) [18] discussed various cyber-attacks related to a healthcare IoT-based infrastructure. They categorized the threats based on their occurrence and clearly described various attacks, pointing to their distinct characteristics. Ahmed *et al*. (2018) [19] discussed malicious insider attacks in multi-cloud-based e-healthcare systems. The multi-cloud environment provides a wide range of services for IoT systems and is also vulnerable due to the heterogeneity in working strategies. Malicious insiders are those who take up a role in the environment but misuse it for some benefit. It can also be those agents who put up some actions unknowingly. In the case of the healthcare environment, these can include both service personnel and the persons from the patients' end. This might lead to manipulation of the sensed data and thereby, a false analysis.

In this section, we consolidated various works discussing the types of attacks against IoT systems. The occurrence of such attacks can result in consequences of varying impacts, according to the application domain (Table **2**).

Table 2. Inferences from 2.2.

References	Inferences	Gaps Identified
[14 - 19]	Various modes of attacks were identified. The patterns in attacks, the consequences and some ideas on how to mitigate these attacks were discussed.	The articles fail to provide a solution that is quick enough to detect, prevent and protect healthcare networks from attacks.

2.3. Privacy Concerns

In their article, Khatkar*et al*. (2020) [20] discussed in detail the impacts of distributed denial of service attacks on healthcare devices. They classified DDOS attacks into five groups based on the motto of the attacker. The limited resource and capacity constraints of IoT systems make them prone to DDOS attacks. Hence, using inherent security frameworks in IoT systems is of prime importance. Sethuraman *et al*. (2020) [21] explained how healthcare IoT devices are hacked and malfunctioned using UAVs. Attack modes like de-authentication attacks, stepping stone attacks, evil twin attacks, WiFi-phishing attacks, *etc*., are also discussed. They also provided an experimental setup to substantiate their findings.

Pu (2020) [22] performed an extensive study on RPL-based security for IoT. The vulnerabilities were analyzed. Then, a GINI-based solution was proposed to prevent Sybil attacks. However, the solution failed to incorporate protection against spoofing attacks. Goel *et al*. (2019) [23] discussed various attacks against IoT systems, suggested some methods to enhance security, and also explained various security paradigms in this context.

In this section, we reviewed various articles that addressed challenges to the privacy of contained data. Preserving the privacy of sensitive data is of great importance as the impact of a possible data breach would include defaming, misuse, *etc*. Healthcare data is sensitive in nature, and protecting the privacy of such medical data is a critical task (Table **3**).

Table 3. Inferences from 2.3.

References	Inferences	Gaps Identified
[20 - 23]	A better understanding of privacy concerns in healthcare networks and the necessity of securing the privacy of data.	The articles discussed only the conventional encryption and intrusion detection methods to preserve data privacy.

2.4. Countermeasures

He *et al*. (2018) [24] presented in their article the necessity of improving the password-based security mechanism for healthcare devices. They illustrated how password-guessing attacks could compromise healthcare devices and steal healthcare data. They also suggested mechanisms to enhance security by adopting strong passwords and also proposed a password-strengthening mechanism.

In their article, Thilakarathne *et al*. (2021) [25] emphasized the privacy concerns in Medical IoT, focusing on where breaches could occur and why they should be preserved. The scope of privacy and its breaches, the gains of attackers, and also countermeasures to keep privacy intact were discussed in the article.

Ranjith and Mahantesh (2019) [26] conducted a collective analysis of various security mechanisms currently employed in smart healthcare systems. Security mechanisms adopted, like attribute-based access control, lightweight authentication, opportunistic computing, context-based, *etc*., were discussed. Issues like secure authentication, DDoS, inner device authentication, key management, *etc*., were also explained.

Fazeldehkordi *et al*. (2019) [27] performed an extensive case study on the security and privacy aspects of healthcare products. The analysis was carried out based on various criteria like connectivity, protection, *etc*. They selected pacemaker security and privacy as the prime subject of analysis and discovered that their proposed security framework enforced better security and privacy for the pacemaker. However, the chances of spoofing-based attacks and DoS attacks were not properly addressed in the article.

Alladi and Chamola (2020) [28] proposed a solution to enforce security against physical attacks in healthcare IoT networks like tampering and/or replacement of collaborating nodes. They suggested using an advanced protocol that employs physical unclonable functions (PUFs), which enforce session key uniqueness and secrecy.

Rughoobur and Nagowah (2017) [29] formulated a framework that detects replay attacks, where the attacker gets hold of the network traffic, acts as a legitimate sender and sends modified packets to the receiver. The framework is formulated using a combination of universally unique identifiers, timestamps and a self-learning battery depletion rate monitor. However, the denial of service attacks was not addressed.

Ge *et al*. (2019) [30] elaborated on a deep learning-enabled solution to detect intrusions in IoT networks. They used the BoT – IoT dataset to retrieve the network-related information and train the system. Features were extracted from the field information and processed to identify potential intrusions.

Vithanwattana *et al*. (2021) [31] suggested a new security framework to enhance the security and privacy of the contained information in healthcare systems. It offered some key services, like encryption as a service, capabilities or tokens to do specific tasks, a storage management system, digital filters to restrict access levels, secure modes of transport and transaction, *etc*. (Table **4**).

Various countermeasures have been proposed for attacks against IoT devices, particularly in the healthcare domain. The need to enhance current security mechanisms was discussed in all the articles.

3. ANALYSIS AND INFERENCES

This section presents a consolidated description of our inferences after reviewing the current trends in healthcare IoT security mechanisms. We analyzed articles published in the past 5 years on related topics. The section is organized in a sequential mode to give a better understanding to the reader. We will first examine the attack patterns over healthcare IoT networks and the strength of existing methods and then discuss them in terms of deep learning-enabled technologies. The subsections are arranged accordingly.

3.1. Attacks over Healthcare IoT

Fig. (**1**) gives an analysis of the occurrences of various network attacks. Tables **5a** and **b** presents the consolidated hierarchical outlook of attacks aimed on healthcare IoT systems. According to recent surveys, 42 percent of these attacks were over or through the network, 33 percent over physical devices and controllers, and the remaining through other modes of attacks.

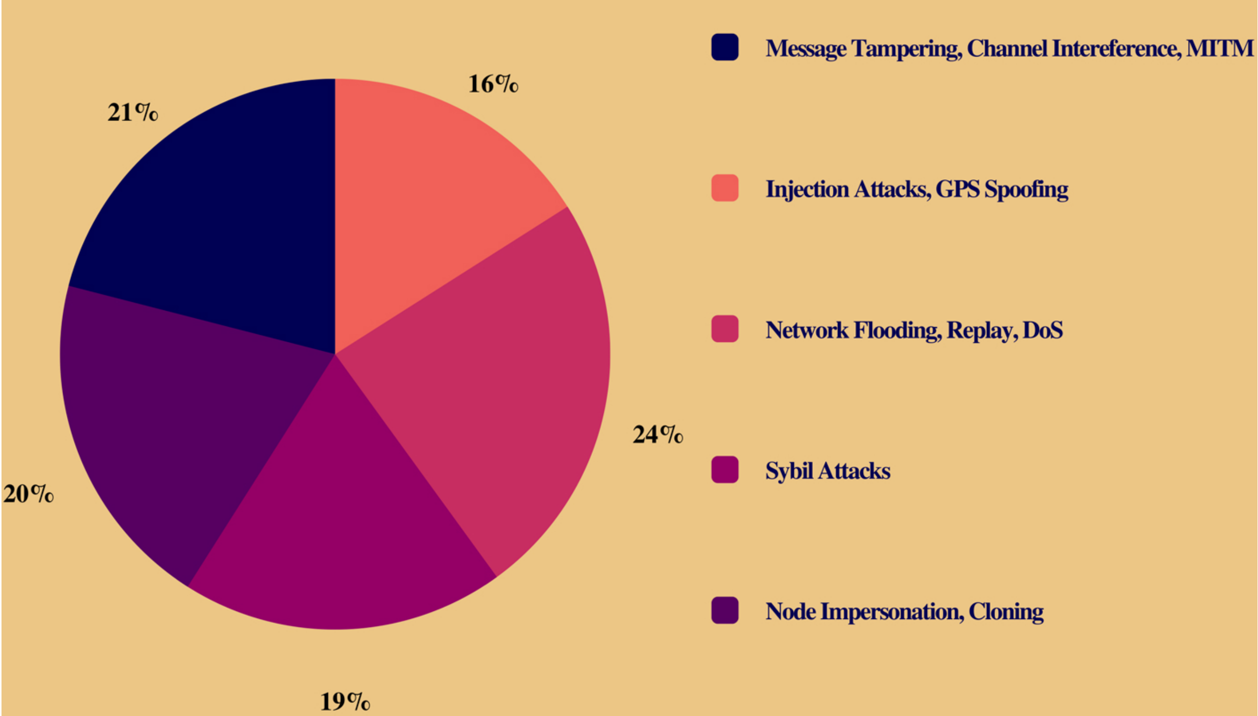

Fig. (1). Network Attacks – Occurrence Pattern.

Table 4. Inferences from 2.4.

References	Inferences	Gaps Identified
[24 - 31]	Recent enhancements in security measures to protect IoT networks are examined. The efficiency of such mechanisms is discussed.	The articles focused only on securing against a specific mode of attack. They did not analyze the possibilities of combined attacks.

Table 5a. Hierarchy of attacks based on the area of attacks.

Attacks on Healthcare IoT devices	**Area of Attacks**	Physical Layer	Malware, RFID spoofing, cloning, physical damage/ alteration
		DataLink Layer	Traffic analysis, MITM, DoS, spoofing, cloning
		Network Layer	IP attacks, sniffing
		Application Layer	Session hijacking, XSS, SQL injection, HTTP-based attacks

Table 5b. Hierarchy of attacks based on the target of attacks.

Attacks on Healthcare IoT devices	**Target of Attacks**	Access	Spoofing, password attacks, cloning
		Data	Phishing, sniffing, social engineering, cryptanalysis
		Controllers	Tampering, DoS, DDoS, jamming, node-based injections
		Networks	Replay attacks, Sybil attacks, IPv6 attacks, MiTM, Network Visualization

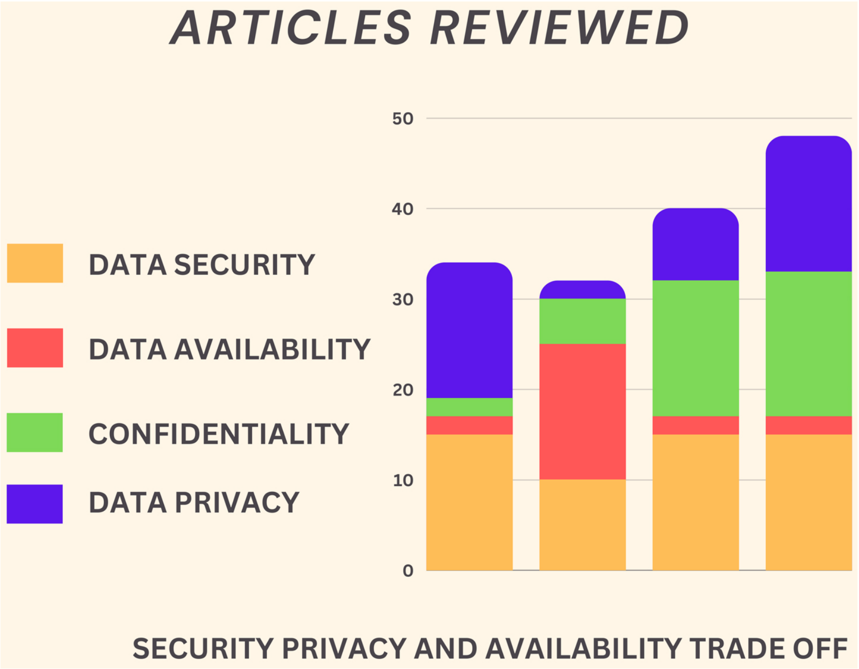

Fig. (2). Articles and parameters.

3.2. Analyzing Current Security Solutions

Fig. (**2**) illustrates the current solutions proposed to protect the HIoT systems.

It indicates whether a particular solution offers the key features of confidentiality, data privacy and availability. These broad classifications will include the integrity of the system and its contained information, availability of the service, authenticity and authorized access.

The articles reviewed in this work addressed one or more of the security concerns in healthcare IoT. However, network attacks in the majority need better attention, and the sensitive information contained demands quick responses.

3.3. Why Use Deep Learning-Based Solutions?

Deep learning is a new artificial intelligence method, which employs algorithms over multiple layers of neural networks. Unlike machine learning, deep learning uses both structured and unstructured learning to build the system, thus providing better accuracy in its predictions. Deep learning has found its application in the healthcare domain in various ways like early disease detection, human behavior recognition, smart device-based detection and analysis of vitals, medicine recognition, *etc*. However, its applications in the security part of healthcare IoT are minimal.

Deep learning emerged as a promising research area in the past decade. The accuracy levels of deep learning compared to that of machine learning have contributed more to its increased popularity and acceptance. The security measures supported by deep learning include detection, analysis, and prevention. By incorporating deep learning in securing IoT systems, we can enforce better privacy of contained information. Fig. (**3**) compares the performances of deep learning and machine learning in security aspects.

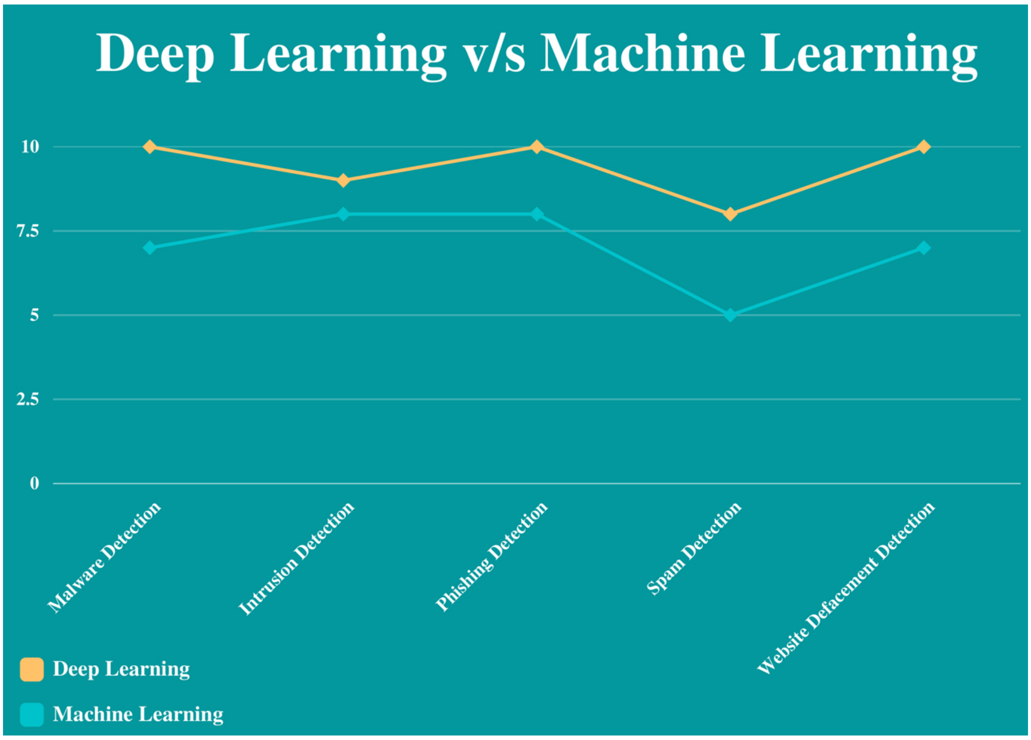

Fig. (3). Accuracy of deep learning and machine learning in security applications.

We could find only a few articles [31 - 39] addressing the security concerns of IoT using deep learning. The primary goals of security, like confidentiality, availability and privacy of the data, are addressed in different articles, but not all in one. The modern modes of network attacks, like distributed denial of service, spoofing, *etc*., are to be tackled well [40 - 47]. The network-related attacks have to be addressed systematically owing to the lethality of consequences if found successful. This can range from the wrong diagnosis to even the death of a patient.

As shown in Fig. (**3**), we compared the machine learning and deep learning-based solutions [48 - 55] employed for security and privacy concerns. It was found that deep learning-based solutions had a slightly better performance in all the aspects we had considered. Hence, we suggest deep learning-based systems for better accuracy in the early detection of occurrence, thereby preventing it.

CONCLUSION AND FUTURE WORKS

The healthcare industry has grown long and wide by introducing IoT-enabled devices. The widespread popularity is owed to the ease of use and self-monitoring capacities offered by these smart systems. Attacks targeting healthcare IoT systems have also exponentially increased as a byproduct. The sensitive nature of contained information is the prime reason for attacking healthcare systems. The still incomplete transition from the conventional mode of healthcare operations adds more risk to the data contained in the network. In this work, we conducted a critical review of the security concerns of healthcare IoT. Possible attacks, current countermeasures, limitations, etc [56 - 71]. were studied and analyzed. We reviewed the recent articles published in this area and found that deep learning-based intelligent applications also have to address the security part of the system, thus enhancing its efficiency. The works addressing security concerns fail to provide a holistic solution. Hence, we have identified the necessity of such a system that can act as a healthcare monitor and support mechanism, along with an added security feature that helps to safeguard the data.

Securing healthcare and other sensitive networks has always been an interesting topic for researchers. The currently available security mechanism has an extensive computation requirement, which counts as an extra overhead. Designing a lightweight yet efficient security framework for healthcare systems has also been proposed by various authors. However, incorporating the capacities of deep learning in securing sensitive healthcare data and networks still needs extensive research. Hence, the proposed future research directions include identifying new pitfalls in network security of healthcare IoT systems, checking the possibilities of employing deep learning to secure the system, and finding out a cost-effective solution that can handle the same. Our future works include designing a suitable security algorithm that helps in quick and prompt authentication for healthcare devices, analyzing the performance and computation trade-off, and then refining our work to provide a lightweight, efficient solution to the security of healthcare IoT devices.

LIST OF ABBREVIATIONS

PUFs	=	Physical Unclonable Functions
RFID	=	Radio-Frequency Identification
DDoS	=	Distributed Denial of Service

CONSENT FOR PUBLICATION

Not applicable.

FUNDING

None.

CONFLICT OF INTEREST

The authors declare no conflicts of interest, financial or otherwise.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] R. Hegde, "Survey on development of smart healthcare monitoring system in IoT environment", *In 2021 5th International Conference on Comp. Method. Commun (ICCMC),* pp. 395-399, 2021.

[2] H. Habibzadeh, K. Dinesh, O. Rajabi Shishvan, A. Boggio-Dandry, G. Sharma, and T. Soyata, "A Survey of Healthcare Internet of Things (HIoT): A clinical perspective", *IEEE Internet Things J.,* vol. 7, no. 1, pp. 53-71, 2020. [http://dx.doi.org/10.1109/JIOT.2019.2946359] [PMID: 33748312]

[3] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved", *IEEE Internet Things J.,* vol. 6, no. 2, pp. 1606-1616, 2019. [http://dx.doi.org/10.1109/JIOT.2018.2847733]

[4] M. Nawir, A. Amir, N. Yaakob, and O.B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks", *In 2016 3rd International Conference on Electronic Design (ICED),* pp. 321-326, 2016. [http://dx.doi.org/10.1109/ICED.2016.7804660]

[5] J. Dofe, A. Nguyen, and A. Nguyen, "Unified countermeasures against physical attacks in internet of things-a survey", *In 2021 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS),* pp. 194-199, 2021. [http://dx.doi.org/10.1109/iSES52644.2021.00053]

[6] R. Kolandaisamy, K. Subaramaniam, and A.B. Jalil, "A study on comprehensive risk level analysis of IoT attacks", *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS),* pp. 1391-1396, 2021. [http://dx.doi.org/10.1109/ICAIS50930.2021.9395858]

[7] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT", *J. Netw. Comput. Appl.,* vol. 149, p. 102481, 2020. [http://dx.doi.org/10.1016/j.jnca.2019.102481]

[8] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y.A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security", *IEEE Internet Things J.,* vol. 7, no. 10, pp. 10250-10276, 2020. [http://dx.doi.org/10.1109/JIOT.2020.2997651]

[9] Z. Mohammad, T. Abu Qattam, and K. Saleh, "Security weaknesses and attacks on the Internet of Things applications", *2019 IEEE Jordan Int Joint Conf Elec Eng Inform Technol (JEEIT),* pp. 431-436, 2019. [http://dx.doi.org/10.1109/JEEIT.2019.8717411]

[10] C. Cilleruelo, J. Junquera-Sánchez, L. de-Marcos, N. Logghe, and J-J. Martinez-Herraiz, "Security and privacy issues of data-over-sound technologies used in IoT healthcare devices", *In 2021 IEEE Globecom Workshops (GC Wkshps).,* pp. 1-6, 2021.

[11] D. Ali, and A. Mahmoud, "Security assessment of internet of things in healthcare environment", *2019 International Conference on Computing and Information Science and Technology and Their Applications (ICCISTA),* pp. 1-6, 2019. [http://dx.doi.org/10.1109/ICCISTA.2019.8830663]

[12] R. Somasundaram, and M. Thirugnanam, "Review of security challenges in healthcare internet of things", *Wirel. Netw.,* vol. 27, no. 8, pp. 5503-5509, 2021. [http://dx.doi.org/10.1007/s11276-020-02340-0]

[13] D.M. Ali, and A.S. Mahmoud, "Internet of things security assessment in healthcare environment", *2019 International Conference on Advances in the Emerging Computing Technologies (AECT),* pp. 1-4, 2020. [http://dx.doi.org/10.1109/AECT47998.2020.9194216]

[14] G. Rajendran, RS. Nivash, P.P. Parthy, and S. Balamurugan, "odern security threats in the Internet of Things (IoT): Attacks and Countermeasures", *2019 International Carnahan Conference on Security Technology (ICCST),* pp. 1-6, 2019.

[15] K. Sharma, "Internet of healthcare things security vulnerabilities and jamming attack analysis", *Expert Syst.,* vol. 39, no. 3, p. e12853, 2022. [http://dx.doi.org/10.1111/exsy.12853]

[16] J. Calvillo-Arbizu, I. Román-Martínez, and J. Reina-Tosina, "Internet of things in health: Requirements, issues, and gaps", *Comput. Methods Programs Biomed.,* vol. 208, p. 106231, 2021. [http://dx.doi.org/10.1016/j.cmpb.2021.106231] [PMID: 34186337]

[17] Y.A. Qadri, R. Ali, A. Musaddiq, F. Al-Turjman, D.W. Kim, and S.W. Kim, "The limitations in the state-of-the-art counter-measures against the security threats in H-IoT", *Cluster Comput.,* vol. 23, no. 3, pp. 2047-2065, 2020. [http://dx.doi.org/10.1007/s10586-019-03036-7]

[18] A. Djenna, and D.E. Saïdouni, "Cyberattacks classification in IoT-based-healthcare infrastructure", *In 2018 2nd Cyber Security in Networking Conference (CSNet),* pp. 1-4, 2018.

[19] A. Ahmed, R. Latif, S. Latif, H. Abbas, and F.A. Khan, "Malicious insiders attack in IoT based Multi-Cloud e-Healthcare environment: A Systematic Literature Review", *Multimedia Tools Appl.,* vol. 77, no. 17, pp. 21947-21965, 2018. [http://dx.doi.org/10.1007/s11042-017-5540-x]

[20] M. Khatkar, K. Kumar, and B. Kumar, "An overview of distributed denial of service and internet of things in healthcare devices", *2020 Research, Innovation, Knowledge Management and Technology Application for Business Sustainability.,* pp. 44-48, 2020.

[21] S.C. Sethuraman, V. Vijayakumar, and S. Walczak, "Cyberattacks on healthcare devices using unmanned aerial vehicles", *J. Med. Syst.,* vol. 44, no. 1, p. 29, 2020. [http://dx.doi.org/10.1007/s10916-019-1489-9] [PMID: 33236166]

[22] C. Pu, "Sybil attack in RPL-based internet of things: analysis and defenses", *IEEE Internet Things J.,* vol. 7, no. 6, pp. 4937-4949, 2020. [http://dx.doi.org/10.1109/JIOT.2020.2971463]

[23] A.K. Goel, A. Rose, J. Gaur, and B. Bhushan, "Attacks, countermeasures and security paradigms in IoT", *In 2019 2nd international conference on intelligent computing, instrumentation and control technologies (ICICICT),* vol. 1, pp. 875-880, 2019. [http://dx.doi.org/10.1109/ICICICT46008.2019.8993338]

[24] D. He, R. Ye, S. Chan, M. Guizani, and Y. Xu, "Privacy in the internet of things for smart healthcare", *IEEE Commun. Mag.,* vol. 56, no. 4, pp. 38-44, 2018. [http://dx.doi.org/10.1109/MCOM.2018.1700809]

[25] N.N. Thilakarathne, "Privacy dilemma in healthcare: A review on privacy preserving medical internet of things", *In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT),* pp. 1-10, 2021.

[26] J. Ranjith, and K. Mahantesh, "Privacy and Security issues in Smart Health Care", *In 2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT),* pp. 378-383, 2019. [http://dx.doi.org/10.1109/ICEECCOT46775.2019.9114681]

[27] E. Fazeldehkordi, O. Owe, and J. Noll, "Security and privacy in IoT systems: A case study of healthcare products", *In 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT),* pp. 1-8, 2019. [http://dx.doi.org/10.1109/ISMICT.2019.8743971]

[28] T. Alladi, V. Chamola, and Naren, "HARCI: A two-way authentication protocol for three entity healthcare IoT networks", *IEEE J. Sel. Areas Comm.,* vol. 39, no. 2, pp. 361-369, 2021. [http://dx.doi.org/10.1109/JSAC.2020.3020605]

[29] P. Rughoobur, and L. Nagowah, "A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare", *In 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS),* pp. 811-817, 2017. [http://dx.doi.org/10.1109/ICTUS.2017.8286118]

[30] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, "Deep learning-based intrusion detection for IoT networks", *In 2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC),* pp. 256-25609, 2019. [http://dx.doi.org/10.1109/PRDC47002.2019.00056]

[31] N. Vithanwattana, G. Karthick, G. Mapp, and C. George, "Exploring a new security framework for future healthcare systems", *In 2021 IEEE Globecom Workshops (GC Wkshps).,* pp. 1-6, 2021.

[32] T. Saba, K. Haseeb, I. Ahmed, and A. Rehman, "Secure and energy-efficient framework using Internet of Medical Things for e-healthcare", *J. Infect. Public Health,* vol. 13, no. 10, pp. 1567-1575, 2020.
[http://dx.doi.org/10.1016/j.jiph.2020.06.027] [PMID: 32682657]

[33] A.K. Sahu, S. Sharma, and R. Raja, "Deep learning-based continuous authentication for an IoT-enabled healthcare service", *Comput. Electr. Eng.,* vol. 99, p. 107817, 2022.
[http://dx.doi.org/10.1016/j.compeleceng.2022.107817]

[34] T. Veeramakali, R. Siva, B. Sivakumar, P.C. Senthil Mahesh, and N. Krishnaraj, "An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model", *J. Supercomput.,* vol. 77, no. 9, pp. 9576-9596, 2021.
[http://dx.doi.org/10.1007/s11227-021-03637-3]

[35] P. Mohamed Shakeel, S. Baskar, V.R. Sarma Dhulipala, S. Mishra, and M.M. Jaber, "Maintaining security and privacy in healthcare system using learning based deep-Q-networks", *J. Med. Syst.,* vol. 42, no. 10, p. 186, 2018.
[http://dx.doi.org/10.1007/s10916-018-1045-z] [PMID: 30171378]

[36] S. Sriram, R. Vinayakumar, M. Alazab, and K. P. Soman, "Network flow based IoT botnet attack detection using deep learning", *In IEEE INFOCOM 2020-IEEE conference on computer communications workshops (INFOCOM WKSHPS),* pp. 189-194, 2020.
[http://dx.doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162668]

[37] T. Aditya Sai Srinivas, and S.S. Manivannan, "Prevention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm", *Comput. Commun.,* vol. 163, pp. 162-175, 2020.
[http://dx.doi.org/10.1016/j.comcom.2020.03.031]

[38] A.R. Khan, M. Kashif, R.H. Jhaveri, R. Raut, T. Saba, and S.A. Bahaj, "Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions", *Secur. Commun. Netw.,* vol. 2022, pp. 1-13, 2022.
[http://dx.doi.org/10.1155/2022/4016073]

[39] L. Aversano, M.L. Bernardi, M. Cimitile, and R. Pecori, "A systematic review on Deep Learning approaches for IoT security", *Comput. Sci. Rev.,* vol. 40, p. 100389, 2021.
[http://dx.doi.org/10.1016/j.cosrev.2021.100389]

[40] S. Paliwal, V. Bharti, and A. K. Mishra, "Changing the outlook of security and privacy with approaches to deep learning", In: *Trends in Deep Learning Methodologies Algorithms, Applications, and Systems,* 2021, pp. 207-226.
[http://dx.doi.org/10.1016/B978-0-12-822226-3.00009-X]

[41] S. Razdan, and S. Sharma, "Internet of Medical Things (IoMT): Overview, emerging technologies, and case studies", *IETE Tech. Rev.,* pp. 1-14, 2021.

[42] A. Thakkar, and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: Recent updates, security issues, and challenges", *Arch. Comput. Methods Eng.,* vol. 28, no. 4, pp. 3211-3243, 2021.
[http://dx.doi.org/10.1007/s11831-020-09496-0]

[43] D. Sparrell, "Cyber-safety in healthcare IoT", *In 2019 ITU kaleidoscope: ICT for health: networks, standards and innovation (ITU K).,* pp. 1-8, 2019.

[44] H. Bolhasani, M. Mohseni, and A.M. Rahmani, "Deep learning applications for IoT in health care: A systematic review", *Informatics in Medicine Unlocked,* vol. 23, p. 100550, 2021.
[http://dx.doi.org/10.1016/j.imu.2021.100550]

[45] Y. Yue, S. Li, P. Legg, and F. Li, "Deep learning-based security behaviour analysis in iot environments: A survey", *Secur. Commun. Netw.,* vol. 2021, pp. 1-13, 2021.
[http://dx.doi.org/10.1155/2021/8873195]

[46] P. D. Singh, G. Dhiman, and R. Sharma, "Internet of things for sustaining a smart and secure healthcare system", *Sustainable computing: Informatics and systems,* vol. 33, p. 100622, 2022.
[http://dx.doi.org/10.1016/j.suscom.2021.100622]

[47] S. Ketu, and P.K. Mishra, "Internet of Healthcare Things: A contemporary survey", *J. Netw. Comput. Appl.,* vol. 192, p. 103179, 2021.
[http://dx.doi.org/10.1016/j.jnca.2021.103179]

[48] H. Ahmadi, G. Arji, L. Shahmoradi, R. Safdari, M. Nilashi, and M. Alizadeh, "The application of internet of things in healthcare: A systematic literature review and classification", *Univers. Access Inf. Soc.,* vol. 18, no. 4, pp. 837-869, 2019.
[http://dx.doi.org/10.1007/s10209-018-0618-4]

[49] P.K. Binu, and M. Kiran, "Attack and anomaly prediction in IoT networks using machine learning approaches", *2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT),* pp. 1-6, 2021.

[50] P. Kamble, and A. Gawade, "Digitalization of healthcare with iot and cryptographic encryption against dos attacks", *In 2019 International Conference on contemporary Computing and Informatics (IC3I),* pp. 69-73, 2021.
[http://dx.doi.org/10.1109/IC3I46837.2019.9055531]

[51] A. Yahyaoui, H. Lakhdhar, T. Abdellatif, and R. Attia, "Machine learning based network intrusion detection for data streaming IoT applications", *In 2021 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter),* pp. 51-56, 2021.
[http://dx.doi.org/10.1109/SNPDWinter52325.2021.00019]

[52] E. Luo, M.Z.A. Bhuiyan, G. Wang, M.A. Rahman, J. Wu, and M. Atiquzzaman, "Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems", *IEEE Commun. Mag.,* vol. 56, no. 2, pp. 163-168, 2018.
[http://dx.doi.org/10.1109/MCOM.2018.1700364]

[53] A. Kore, and S. Patil, "Reliable and secure data transmission in smart healthcare application of internet of things", *2021 IEEE Bombay Section Signature Conference (IBSSC),* pp. 1-6, 2021.
[http://dx.doi.org/10.1109/IBSSC53889.2021.9673462]

[54] R. Marshal, K. Gobinath, and V.V. Rao, "Proactive measures to mitigate cyber security challenges in IoT based smart healthcare networks", *Electronics and Mechatronics Conference (IEMTRONICS),* pp. 1-4, 2021.

[55] P.K. Dhillon, and S. Kalra, "Multi-factor user authentication scheme for IoT-based healthcare services", *J. Reliab. Intell. Environ.,* vol. 4, no. 3, pp. 141-160, 2018.
[http://dx.doi.org/10.1007/s40860-018-0062-5]

[56] S. Sahoo, S.S. Sahoo, B. Sahoo, and A.K. Turuk, "Design of an Authentication Scheme for Cloud-Based IoT Applications", *IETE Tech. Rev.,* pp. 1-14, 2021.

[57] X. Guo, H. Lin, Y. Wu, and M. Peng, "A new data clustering strategy for enhancing mutual privacy in healthcare IoT systems", *Future Gener. Comput. Syst.,* vol. 113, pp. 407-417, 2020.
[http://dx.doi.org/10.1016/j.future.2020.07.023]

[58] H.K. Bharadwaj, A. Agarwal, V. Chamola, N.R. Lakkaniga, V. Hassija, M. Guizani, and B. Sikdar, "A review on the role of machine learning in enabling IoT based healthcare applications", *IEEE Access,* vol. 9, pp. 38859-38890, 2021.
[http://dx.doi.org/10.1109/ACCESS.2021.3059858]

[59] P. Gope, Y. Gheraibia, S. Kabir, and B. Sikdar, "A secure IoT-based modern healthcare system with fault-tolerant decision making process", *IEEE J. Biomed. Health Inform.,* vol. 25, no. 3, pp. 862-873, 2021.
[http://dx.doi.org/10.1109/JBHI.2020.3007488] [PMID: 32749985]

[60] S. Singh, and D. Kumar, "An efficient use of privacy preserving resources in IoT based healthcare", *In 2021 10th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks (IEMECON),* pp. 1-5, 2021.
[http://dx.doi.org/10.1109/IEMECON53809.2021.9689201]

[61] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices", *IEEE Internet Things J.,* vol. 6, no. 5, pp. 8182-8201, 2019.
[http://dx.doi.org/10.1109/JIOT.2019.2935189]

[62] S.S. Gopalan, A. Raza, and W. Almobaideen, "Iot security in healthcare using AI: A survey", *In 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA),* pp. 1-6, 2021.
[http://dx.doi.org/10.1109/ICCSPA49915.2021.9385711]

[63] S. Nasiri, F. Sadoughi, M. Tadayon, and A. Dehnad, "Security requirements of internet of things-based healthcare system: A survey study", *Acta Inform. Med.,* vol. 27, no. 4, pp. 253-258, 2019.
[http://dx.doi.org/10.5455/aim.2019.27.253-258] [PMID: 32055092]

[64] B. Liao, Y. Ali, S. Nazir, L. He, and H.U. Khan, "Security analysis of IoT devices by using mobile computing: A systematic literature review", *IEEE Access,* vol. 8, pp. 120331-120350, 2020.
[http://dx.doi.org/10.1109/ACCESS.2020.3006358]

[65] S. El-Gendy, and M.A. Azer, "Security Framework for Internet of Things (IoT)", *In 2020 15th International Conference on Computer Engineering and Systems (ICCES),* pp. 1-6, 2020.

[66] S. Masengo Wa Umba, A.M. Abu-Mahfouz, and D. Ramotsoela, "Artificial intelligence-driven intrusion detection in software-defined wireless sensor networks: towards secure IoT-Enabled healthcare systems", *Int. J. Environ. Res. Public Health,* vol. 19, no. 9, p. 5367,

2022.
[http://dx.doi.org/10.3390/ijerph19095367] [PMID: 35564763]

[67] N. Sivasankari, and S. Kamalakkannan, "Detection and prevention of man-in-the-middle attack in iot network using regression modeling", *Adv. Eng. Softw.,* vol. 169, p. 103126, 2022.
[http://dx.doi.org/10.1016/j.advengsoft.2022.103126]

[68] M. Saed, and A. Aljuhani, "Detection of man in the middle attack using machine learning", *2022 2nd International Conference on Computing and Information Technology (ICCIT),* pp. 388-393, 2022.
[http://dx.doi.org/10.1109/ICCIT52419.2022.9711555]

[69] M. Masud, G.S. Gaba, K. Choudhary, M.S. Hossain, M.F. Alhamid, and G. Muhammad, "Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare", *IEEE Internet Things J.,* vol. 9, no. 4, pp. 2649-2656, 2022.
[http://dx.doi.org/10.1109/JIOT.2021.3080461]

[70] M. Almulhim, and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications", *In 2018 20th International Conference on advanced communication technology (ICACT),* pp. 481-487, 2018.

[71] R. Geetha, and T. Thilagam, "A review on the effectiveness of machine learning and deep learning algorithms for cyber security", *Arch. Comput. Methods Eng.,* vol. 28, no. 4, pp. 2861-2879, 2021.
[http://dx.doi.org/10.1007/s11831-020-09478-2]