International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Cybersecurity in Healthcare IoT Devices: Studying the Vulnerabilities and Defence Mechanisms for IoT devices used in Healthcare Settings

Vivek Yadav

Email: *yadav.vivek[at]myyahoo.com*

Abstract: ***IoT adoption in the healthcare Industry referred to as the Internet of Medical Things (IoMT) offers a boost towards improving patient care through continuous monitoring and collection of data. It aims at identifying the privacy and security risks which need to be addressed in the context of connected healthcare IoT devices. It will involve trying to regularly analyse network traffic data and establish the patterns associated with it. This method includes using the secondary data from sources including Kaggle and applying machine learning using Python including the K - means clustering models and ARIMA models to expose variability as well as prospecting cyber threats in the network traffic. There is a dire need for improving security measures like secure data encryption, optimum authentication techniques and constant network monitoring. The findings on personnel and device vulnerability confirm that healthcare organizations must implement a strong preventive strategy to safeguard patient information and confidence in medical equipment. The healthcare IoT should adopt both symmetric and asymmetric encryptions, as well as artificial intelligence security solutions to contain threats and enhance safety against cyber threats.***

Keywords: Internet of Things (IoT), Internet of Medical Things (IoMT), Cybersecurity threats, Message Queuing Telemetry Transport (MQTT), defence mechanisms, Healthcare

1. Introduction

IoT devices are used to exchange and collect data to maintain data processing and gain information about business transformation. In the healthcare sector, IoT devices have been used to maintain patient care, monitor information, and collect real - time data. Applications related to the “Internet of Things” (IoT) health care are crucial because they include data processing or storage that requires extremely high security [1]. The advancements of IoT devices in the healthcare sector increase the cybersecurity risks that reduce the efficiency of the business process. The health and well - being of billions of people worldwide will undoubtedly be significantly impacted by the “Internet of Medical Things” (IoMT) or the “Internet of Healthcare Things” (IoHT). Wireless implanted medical devices are seeing a sharp increase in their use, applications, and complexity due to the widespread use of internetworking technologies like the MIoT [2]. Insulin pumps, wearable sensors, and other activities are used increasingly in healthcare and the insufficient security, as well as the critical nature of the devices, enhances the cyberattacks. Medical data is far more sensitive and significant than financial data; however, security measures in the healthcare industry are given less attention than in the finance sector [3]. Unauthorised access, disruption of essential healthcare services, and unauthorised access can increase vulnerabilities in the healthcare system. A Simple IoT cloud - based system is provided, that can monitor wearables in a low - power, rechargeable and lightweight way utilising an ECG sensor, temperature sensor, and magnetic field detector to analyse the ECG signal, heart rate and temperature patient [6]. This is linked to a monitoring system via a fast, low - power WiFi connection that will send data instantly to the cloud. Radiofrequency (RF) devices have a low attack probability since the attack must be carried out in close proximity to the patient. Follow - up appointments in the hospital involve the activation of the radiofrequency function [7]. In order to do an attachment, a patient must have short - range access with active radiofrequency functionality. Every wireless device's frequency can be easily found online by searching for the Federal Communications Commission ID (FCC ID). The capacity to read and write to any legitimate memory address on the device could be the outcome of a successful radio frequency scan.

Aim

The aim of the study is to examine the network traffic data to understand the cyberattacks faced by the healthcare sector's IoT devices, as well as determine the defence mechanisms to increase security.

Objectives

- To analyse the patterns of the network traffic that are associated with healthcare IoT devices, focusing on communication flows, port usage, and IP addresses
- To evaluate the potential security threats and anomalies behaviour in the network traffic
- To implement K - means algorithms for understanding the structures and patterns of the network behaviours
- To provide an effective security framework for healthcare IoT devices

2. Literature Review

2.1 Exploring Security and privacy problems with IoT in healthcare

Applications for healthcare are extremely important, and medical data is more complicated and sensitive to security than other types of data and applications since it must be extremely secure. The ability of an Internet of Things (IoT) to be remotely managed over an existing network infrastructure presents a chance for more direct device integration with computer - based processes, leading to increased accuracy and efficiency. Adopting preventative or essential measures

to enhance an individual's well - being is referred to as healthcare [16]. This can be accomplished through surgery, medication administration, or other lifestyle modifications. The health care system, which is composed of hospitals and doctors, usually provides these services. Healthcare providers and patients will both gain from the growing use of IoT in the industry. The remote monitoring and communication capabilities of IoT can significantly improve the quality of treatments that patients get [4]. A modern pacemaker has the ability not only to store data about patients but also share it via the WiFi to an access point, or some medical equipment used during the examination in a hospital. The wireless node devices, that maintain data related to patient's health activities at home send this information to central servers. Pacemakers with the facility for transferring data through the Internet are useful in those patients with limited mobility [5]. However, the data communications used while transferring the data to other external servers are relatively simple and can easily be stolen. In the healthcare system, an insulin pump is used to improve patient care using IoT devices and hackers can exploit the overdose issue [18]. The effective technology can be vulnerable as the communications of the technologies are not encrypted from accessing the devices.

2.2 Analysing the importance of defence mechanism

Technology refers to the application of scientific knowledge for the use of real - life resources and the integration of IoT devices in healthcare has led to improved patient care through real - time monitoring of the patient, data collection, and remote analysis. However, the usage of or incorporation of these facilities has also brought new and significant cybersecurity threats. The necessity to ensure the protection of the defence mechanisms of healthcare IoT devices should not be underestimated since interference with healthcare data could have severe consequences for human lives, and it may also lead to interruptions in the provision of medical services [8]. Many healthcare IoT devices (from various categories) deal with health - related data both, those belonging to identifiable patients and their physiological data in real - time. Any compromise on this type of data can result in a major violation of patients' rights to privacy and confidentiality, and extortionate loss of their money to fraudsters [19]. Furthermore, healthcare cyber - attackers may take a proactive tactic over the infected IoT devices and make them produce wrong outputs or simply fail, by giving an inaccurate diagnosis or recommendations that may harm the patient [9]. These risks require countermeasures in that appropriate defence mechanisms must be adopted to avoid adverse consequences. It includes secure data encryption to enhance the security of the data in transit, optimum authentication procedures that unauthorized access, and constant surveillance of the network to check for breaches and respond to them in the shortest time possible. Such measures prove useful in the protection of patient information, increased trust in health - related equipment, and fostering a positive image in the delivery of health care services.

2.3 Literature gap

The study focuses on cybersecurity in healthcare IoT and it has been seen that a gap has been created in understanding the network behaviour and the patterns of the network traffic. The lack of effective framework that enhances effective machine - learning techniques for mitigating and detecting the network traffic data in this study. Additionally, the main aim of the study is to determine the gap by evaluating the network traffic data and improving the targeted defence mechanisms.

3. Methodology

3.1 Data collection and analysis

Secondary data collection methods have been used to explore cybersecurity attacks based on the healthcare IoT. The primary goal is to identify and evaluate the merits and demerits of research procedures, including both qualitative and quantitative approaches, using secondary data or sources [10]. Relevant research studies and datasets have been gathered to explore the treatment process in the healthcare sector. Kaggle is an effective data source that can be used to collect the relevant data based on the vulnerability, as well as the defence mechanism. The quantitative method has been used to explore cybersecurity vulnerability and collect information based on the defence mechanism. Python programming language has been implemented to gather data regarding the cybersecurity threats of the healthcare IoT device. Moreover, machine learning algorithms have been implemented to explore the potential threats and patterns of network traffic in the healthcare environment.

3.2 Cybersecurity Framework in Healthcare

A robust framework for cyber security in healthcare IoT devices is essential to secure patient's sensitive data. It is also applicable to maintain the reliability of the devices that are used in patient monitoring as well as treatment. Implementation of such a framework is necessary for the healthcare sector as it possesses information of high monetary and intelligence. The data which is targeted the most includes "personality identifying information" (PII) or "protected health information" (PHI).

Implementation of the k - means clustering for checking the anomalies is unparalleled because the unsupervised machine learning algorithm can group the unlabelled dataset into different clusters. Another framework based on symmetric key encryption can be followed in the healthcare sector [17]. "Advanced Encryption Standards" are among the commonly used algorithms that use the same key for both encryption and decryption.

$T = Ke (Ct)$

$Ct = Kd (T)$

The process is executed using the above expression in which T, Ke, Ct and Kd represent the original message, encryption key, ciphered message and decryption key respectively. The MQTT messages along with other packets can be hidden with the help of an asymmetric encryption process. In this process, the entire activities are executed using two different keys. On the other hand, healthcare authorities can adapt to a hybrid encryption process by combining the strengths of both symmetric as well as asymmetric encryption.

4. Results and Discussion

4.1 Results

The results section is made of different sections starting from "Exploratory Data Analysis" (EDA) followed by clustering and ARIMA analysis. EDA is necessary for the analysis to identify the dataset in a more suitable and interpretable manner so that the hidden patterns from the data can easily be understood [13]. The analysis consists of descriptive analysis and explores different aspects of "Message Queuing Telemetry Transport" (MQTT).

Descriptive statistics of numerical columns:

	frame.time_delta	frame.time_relative	frame.len	tcp.srcport	tcp.dstport	tcp.time_delta	tcp.len	tcp.ack
count	76810.000000	76810.000000	76810.000000	76810.000000	76810.000000	76810.000000	76810.000000	76810.000000
mean	0.133703	2921.691253	79.308449	37652.780029	4098.876500	3.501738	11.308449	637.383244
std	0.464622	1891.546099	14.766326	9866.519362	8897.447631	9.752309	14.766326	3793.878933
min	0.000000	0.000000	70.000000	1883.000000	1883.000000	0.000000	2.000000	1.000000
25%	0.000035	1314.960131	77.000000	35965.000000	1883.000000	1.995325	9.000000	51.000000
50%	0.000087	2712.962844	78.000000	38937.000000	1883.000000	1.999715	10.000000	99.000000
75%	0.000180	4479.037043	80.000000	42449.000000	1883.000000	2.002226	12.000000	165.000000
max	2.155548	6611.038212	1766.000000	46801.000000	46801.000000	60.037328	1698.000000	59658.000000

Figure 1: Descriptive statistics

The descriptive statistics of the columns containing only numerical values have been displayed in the image above. The statistics consist of mean, standard deviation, maximum and minimum values along with percentiles.

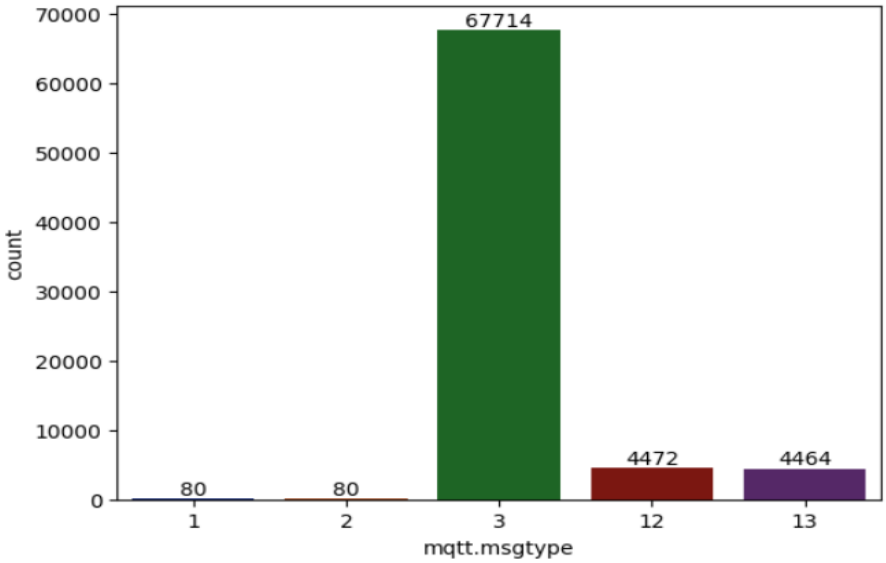

Figure 2: Different types of MQTT messages

The above column plot shows different types of MQTT messages that are used to demonstrate various operational states in healthcare. Type "3" messages have been transferred the most compared to the other four. The unusual message patterns can be identified through this process which may eventually indicate malicious activities.

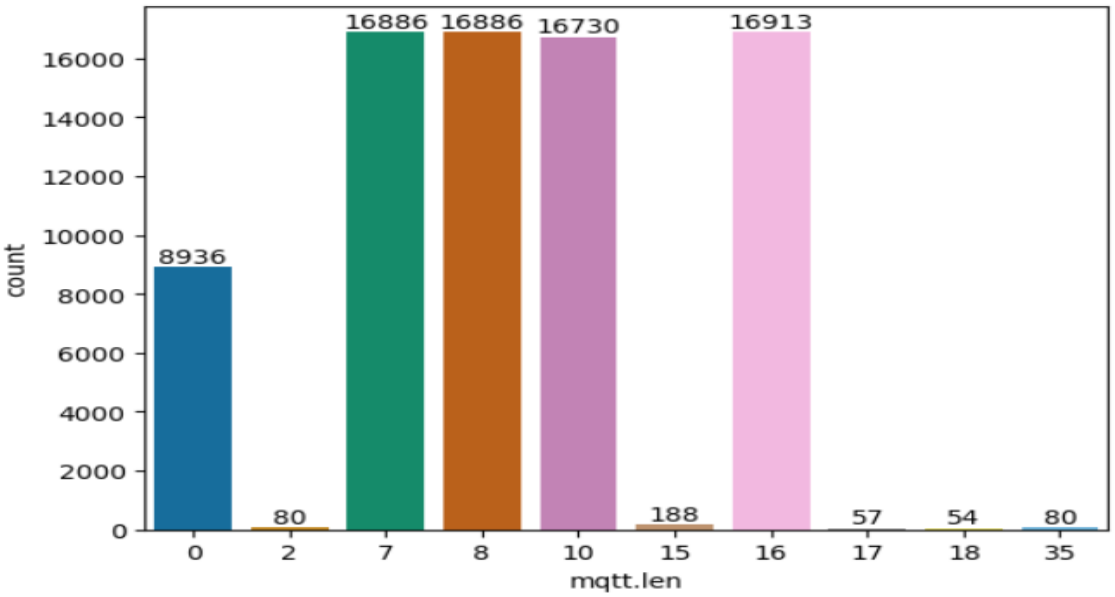

Figure 3: Different lengths of the messages

The above image analyses the distribution of the message lengths based on the dataset, which displays that most messages are 7, 8, 10 and 16 units long. The typical MQTT message lengths are normally consistent in healthcare IoT networks [14]. The presence of unusually long messages indicates the possibility of probing activities as well as data exfiltration.

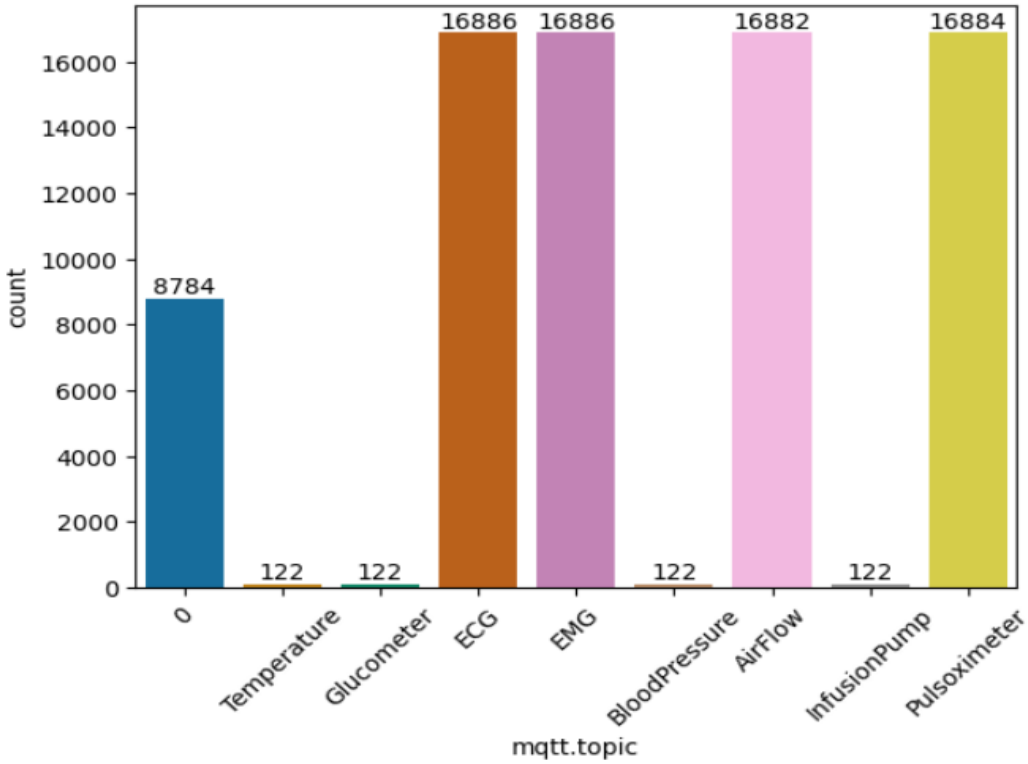

Figure 4: Topics of the messages

The above bar plot indicates the topic of the messages related to different healthcare entities. As per the plot, the maximum number of messages are regarding ECG and EMS, followed by infusion pump and pulse oximeter.

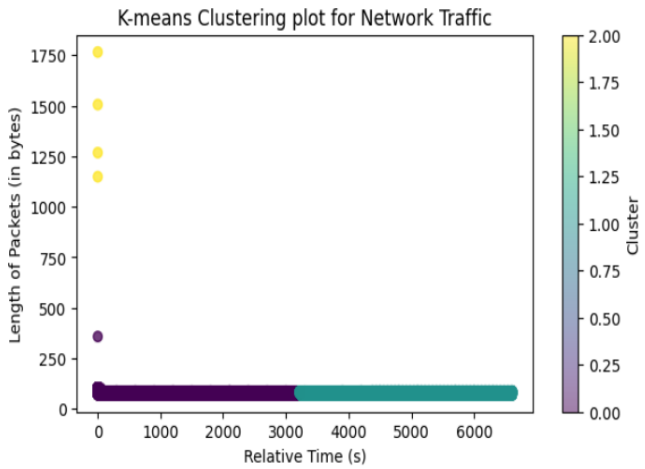

Figure 5: K - means clustering plot

The results of the K - means clustering demonstrating the network traffic have been displayed in the above image. The k - means clustering is applied to gain valuable insights regarding the behaviour as well as structure of traffic in the environment of healthcare IoT [15]. The scatter plot indicates that the traffic contains small packets mostly whereas some larger packets can also be noticed.

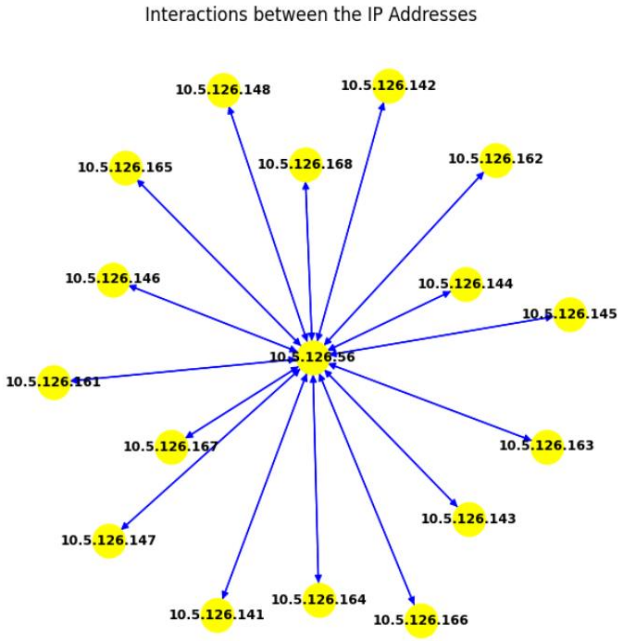

Figure 6: Interaction between different IP addresses

The communication pattern along with the network structure of healthcare IoT devices is represented in the image above. It indicates the source and destination IP addresses to identify normal as well as abnormal behaviours in the network.

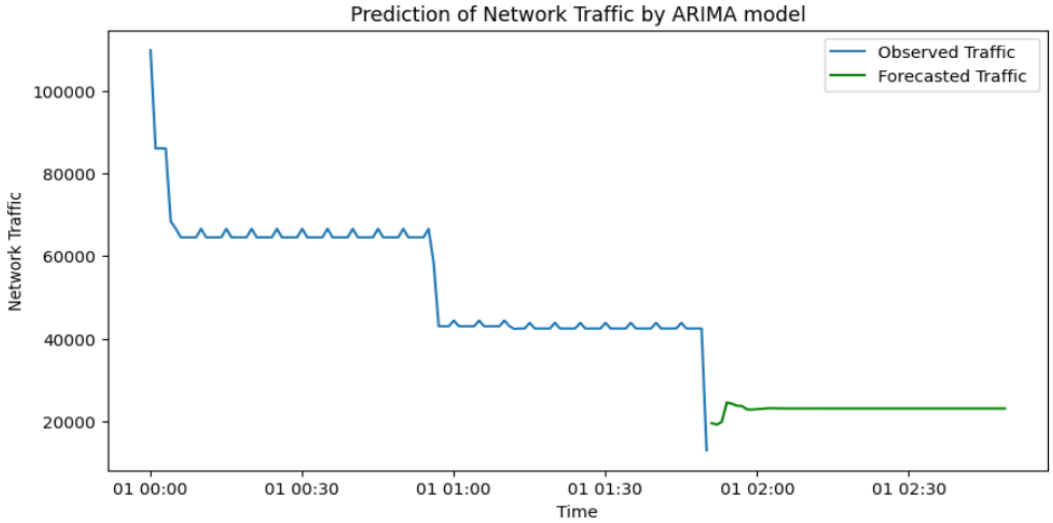

Figure 7: Network prediction for the next 60 seconds

An "Auto Regressive Integrated Moving Average" or ARIMA model has been developed in this section to predict the traffic in the network. The above line plot forecasts the traffic for the next 60 seconds along with displaying the observed traffic as well.

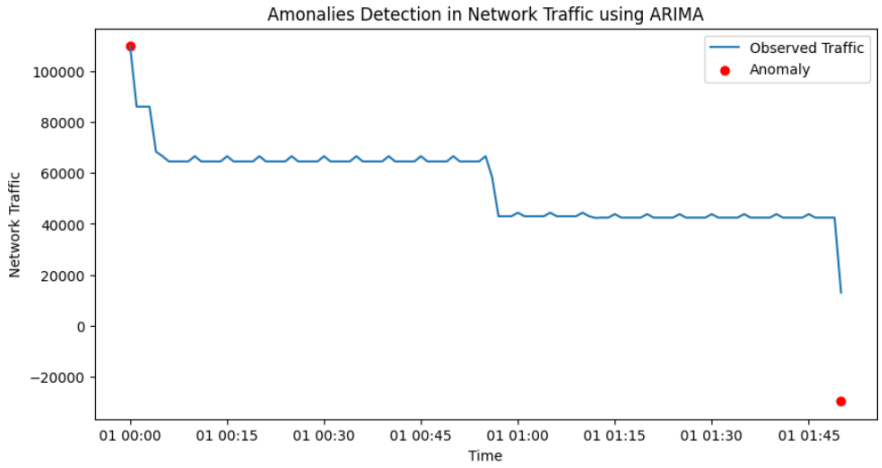

Figure 8: Anomaly detection in the traffic

The above line plot displays the observed network traffic along with the presence of an anomaly. Anomalies have been detected at the very beginning and end of the observed traffic. These are required to be identified as early as possible so that data breaches, cyber - attacks and many more can be predicted and avoided.

4.2 Discussion

The results section sheds light on the structure of the network as well as its behaviour in the case of IoT devices. On top of that, it identifies the vulnerabilities present in the network traffic with the help of EDA and cluster analysis. The exploratory data analysis acts as the foundation for further analyses. The basic properties of the dataset are identified with the help of descriptive analysis which is also responsible for providing a basic idea regarding the numerical columns. Various plots regarding the pattern of MQTT messages indicate that there may be some vulnerabilities in the network traffic as the presence of a few unusual messages has been identified. Using sensors like EEG and ECG, the publisher of a smart healthcare system measures blood pressure, heart rate, and other health - related parameters. The publisher then uses MQTT to deliver the data to the subscriber [11]. The results from the k - means clustering highlight that most packets in the network are small in size. The ARIMA model has been used to predict the behaviour of traffic in the next 60 seconds along with anomaly identification. The resultant plots also signify the presence of anomalies in the traffic as per the dataset.

IoT has been accepted as a part of the system by the healthcare communities, thus steps to reduce the IoT risks must be implemented.

Table 1: Possible steps to follow to secure IoT healthcare devices

Steps	Description
Effective authentication method	The connection must be authenticated using digital certificates and public key infrastructure to avoid data manipulation during data package transit.
Continuous assessment	Best security practices such as passwords, encryption and regular backup must be implemented by the healthcare authorities [12].
Segment networks	The connectivity of the devices must be limited along with a proper identification of the IP addresses. The network graph can be a useful tool to monitor the source and destination IP addresses of IoT devices.

Apart from the steps mentioned in the table, based on the analysis results, the implementation of AI can be another approach to cyber security as it enhances security with an absorbed focus on outreach.

5. Conclusions

It can be concluded that the study explored the cybersecurity issues in the healthcare IoT and modern healthcare equipment such as pacemakers, ECG recorders, insulin pumps, and others used in healthcare. The issues of cybersecurity in IoT devices focused on determining the vulnerabilities and defence mechanisms are used to reduce the cybersecurity attack in healthcare services. Real - time data has been used to explore the integration of IoT devices for developing patient care by maintaining an effective monitoring process. Sensitive data of the patients has been stored in the devices and the lack of security measures increases risks. Kaggle has been used to gather data based on the healthcare IoT devices that allow for evaluating the anomalies and patterns of the network traffic. Python language has been used to collect information about the data analysis method, as well as k - means clustering and ARIMA model have been implemented to obtain the vulnerabilities of the network traffic. Additionally, the analysis focused on the defence mechanism by maintaining data encryption, network monitoring, and effective protocols that are used to mitigate the risks of the healthcare sector.

References

[1] Alharam, A. K. and Elmedany, W., 2017, August. Complexity of cyber security architecture for IoT healthcare industry: A comparative study. In *2017 5th international conference on future internet of things and cloud workshops (FiCloudW)* (pp.246 - 250). IEEE.

[2] Jackson Jr, G. W. and Rahman, S., 2019. Exploring challenges and opportunities in cybersecurity risk and threat communications related to the medical Internet of Things (MIoT). *arXiv preprint arXiv: 1908.00666*.

[3] Razaque, A., Amsaad, F., Khan, M. J., Hariri, S., Chen, S., Siting, C. and Ji, X., 2019. Survey: Cybersecurity

vulnerabilities, attacks and solutions in the medical domain. *IEEE Access*, *7*, pp.168774 - 168797.

[4] Chacko, A. and Hayajneh, T., 2018. Security and privacy issues with IoT in healthcare. *EAI Endorsed Transactions on Pervasive Health and Technology*, *4* (14).

[5] Abdul - jabbar, H. M. and Abed, J. K., 2020, March. Real time pacemaker patient monitoring system based on internet of things. In *IOP Conference Series: Materials Science and Engineering* (Vol.745, No.1, p.012093). IOP Publishing.

[6] Yee, R., Verma, A., Beardsall, M., Fraser, J., Philippon, F. and Exner, D. V., 2013. Canadian Cardiovascular Society/Canadian Heart Rhythm Society joint position statement on the use of remote monitoring for cardiovascular implantable electronic device follow - up. *Canadian Journal of Cardiology*, *29* (6), pp.644 - 651.

[7] Longras, A., Oliveira, H. and Paiva, S., 2020, June. Security vulnerabilities on implantable medical devices. In *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)* (pp.1 - 4). IEEE.

[8] Ge, M., Cho, J. H., Ishfaq, B. and Kim, D. S., 2020. Modelling and analysis of integrated proactive defence mechanisms for internet of things. *Modelling and Design of Secure Internet of Things*, pp.217 - 247.

[9] Prates, N., Vergütz, A., Macedo, R. T., Santos, A. and Nogueira, M., 2020, December. A defence mechanism for timing - based side - channel attacks on IoT traffic. In *GLOBECOM 2020 - 2020 IEEE Global Communications Conference* (pp.1 - 6). IEEE.

[10] Choy, L. T., 2014. The strengths and weaknesses of research methodology: Comparison and complimentary between qualitative and quantitative approaches. *IOSR journal of humanities and social science*, *19* (4), pp.99 - 104.

[11] Patel, C. and Doshi, N., 2020. A novel MQTT security framework in generic IoT model. *Procedia Computer Science*, *171*, pp.1399 - 1408.

[12] Blanke, S. J. and McGrady, E., 2016. When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. *Journal of healthcare risk management*, *36* (1), pp.14 – 2

[13] Verbeeck, N., Caprioli, R. M. and Van de Plas, R., 2020. Unsupervised machine learning for exploratory data analysis in imaging mass spectrometry. *Mass spectrometry reviews*, *39* (3), pp.245 - 291.

[14] Liu, X., Zhang, T., Hu, N., Zhang, P. and Zhang, Y., 2020. The method of Internet of Things access and network communication based on MQTT. *Computer Communications*, *153*, pp.169 - 176.

[15] Flora, D. B., LaBrish, C. and Chalmers, R. P., 2012. Old and new ideas for data screening and assumption testing for exploratory and confirmatory factor analysis. *Frontiers in psychology*, *3*, p.55.

[16] Yip, W., Subramanian, S. V., Mitchell, A. D., Lee, D. T., Wang, J. and Kawachi, I., 2007. Does social capital enhance health and well - being? Evidence from rural China. *Social science & medicine*, *64* (1), pp.35 - 49.

[17] Elhoseny, M., Ramírez - González, G., Abu - Elnasr, O. M., Shawkat, S. A., Arunkumar, N. and Farouk, A., 2018. Secure medical data transmission model for IoT - based healthcare systems. *Ieee Access*, *6*, pp.20596 - 20608.

[18] Chacko, A. and Hayajneh, T., 2018. Security and privacy issues with IoT in healthcare. *EAI Endorsed Transactions on Pervasive Health and Technology*, *4* (14).

[19] Flynn, K., 2016. Financial fraud in the private health insurance sector in Australia: Perspectives from the industry. *Journal of Financial Crime*, *23* (1), pp.143 - 158.