Scholars Journal of Engineering and Technology

OPEN ACCESS

Abbreviated Key Title: Sch J Eng Tech
ISSN 2347-9523 (Print) | ISSN 2321-435X (Online)
Journal homepage: https://saspublishers.com

AI-Based Malware Detection in Connected Medical Devices

Gaurang Deshpande[1*]

[1]Software Developer, IBM, USA

DOI: 10.36347/sjet.2023.v11i12.003 | **Received:** 02.11.2023 | **Accepted:** 27.12.2023 | **Published:** 30.12.2023

***Corresponding author:** Gaurang Deshpande
Software Developer, IBM, USA

Abstract | **Original Research Article**

The study focuses AI-based malware detection in connected medical devices. The paper investigates how such vulnerabilities in medical devices that are connected to one another can be reduced through AI-powered malware detection. It examines literature with the technical gaps, ethical issues, and third-party case studies to prove the effectiveness of AI. The study examines the trends in breach using the secondary qualitative and quantitative information and how AI can be used to prevent threats in real-time and adaptively. The results indicate that the number of EMR breaches was over 200 in 2019, whereas IoMT device exposure is on the rise. The research paper finishes by giving recommendations on how to include AI securely and ethically in the healthcare IT infrastructures.

Keywords: Artificial Intelligence (AI), Malware Detection, Internet of Medical Things (IoMT), Cybersecurity, EMR Breaches, Implantable Medical Devices (IMDs).

I. INTRODUCTION

A. Background to the Study

The healthcare sector is revolutionised due to the integration of the "Internet of Medical Things (IoMT)", and this helps to manage the process of different treatments such as patient monitoring, diagnosis, and treatment. Pacemakers, insulin pumps, and ECG Monitors are connected medical equipment that relay real-time data to patient care [1]. Nonetheless, they are connected to the internet, thus vulnerable to the daily activities of hackers, such as malware-based hack. This may be a serious threat to their patient and data security. Old security systems find it hard to track the emerging threats in real-time. This has translated to the increased interest in the use of "artificial intelligence (AI)" based malware detection systems that can provide intelligent, adaptive measures.

B. Overview

The study mainly discussed the application of AI-detected malware on connected medical equipment. Such intelligent gadgets, which constitute the IoMT, are becoming more prevalent in hospitals and home-based care for health monitoring duties. Certainly, they are associated with important medical advantages [2]. However, being connected to the internet, they also present a serious concern related to cybersecurity as well. It is now being deployed on AI and machine learning algorithms that detect deviations in behaviour patterns that might indicate that a malware attack is imminent.

C. Problem Statement

The reliance on interconnected medical devices has brought up new vulnerabilities in the healthcare systems. The traditional malware-detecting strategies do not address the newly formed, inventive cyber threats and cannot respond rapidly to them. Such a cyberattack might trigger life-threatening malfunctions, data decryption, or shutdowns [3]. The main challenge is absence of threat detection by smart and instant programming puts the lives of the patients and hospitals in danger. It is thus urgent to find out how AI-based malware detection technology could offer a proactive, precise, and scalable solution.

D. Aim and Objectives

The aim of the study is to evaluate the AI-based malware detection effectiveness in improving the cybersecurity of medical devices that are connected to healthcare systems. The objectives are: 1. To address the issue of the malware exposure to connected medical devices vulnerability. 2. To identify the effectiveness of AI in identifying malware in real-time. 3. To evaluate the advantages and shortcomings of the adoption of AI-based detection technologies in clinical settings.

E. Scope and Significance

The scope of the study is to focus on malware detection-based AI, in particular, connected medical equipment in hospitals and home care. It looks into the nature of cyber threats that such devices encounter, the prevailing issues concerning the existing traditional security systems, along with how AI offers intelligent, dynamic protection. The significance lies in identifying the importance of the research lies in informing that there is a strong demand in the healthcare technology field to have efficient security systems which are real-time in nature [4]. It provides implications that can assist the healthcare providers, IT specialists, and policymakers in the development of a secure digital infrastructure that will safeguard the lives and sensitive health information of the patients.

II. LITERATURE REVIEW

A. Cybersecurity Challenges in Connected Medical Devices

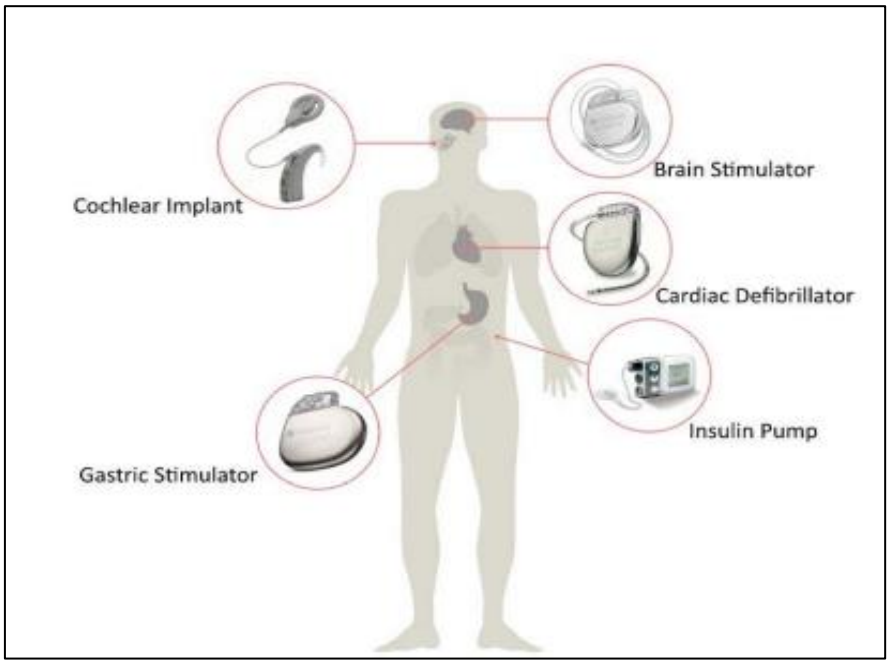

Figure 1: Example of Implantable Medical Devices
(Source: [5])

The aspect to the increasing cybersecurity risk against implantable medical devices (IMDs), pacemakers, defibrillators and neurostimulators. These gadgets are implanted in the body of a patient and equipped with wireless communications with exterior systems to monitor and update information in them [5]. The study focuses on the vulnerability of such life-saving devices to possible cyberattacks through weak encryption, the absence of sufficient authentication, and wireless exploits. The manufacturers, healthcare providers and regulators have to come together to protect the regulatory terrain of smart healthcare. ***[Refer to Figure 1]***

Mainly discussed the issues related to cybersecurity within the medical ecosystem due to the rapid growth of modern technologies. Most of the medical devices do not have strong inbuilt security systems because the design models are old, and this puts them at risk of hacking and malware attacks [6]. They promote risk-based control of cybersecurity at various lifecycle stages of the device, such as design and development, deployment and maintenance. This is also emphasised in the study as the need to have manufacturers, regulators and healthcare providers work together to establish dynamic and adaptable security systems that will be able to respond in real-time to the emerging threats without threatening the safety of patients.

B. Role of AI in Malware Detection

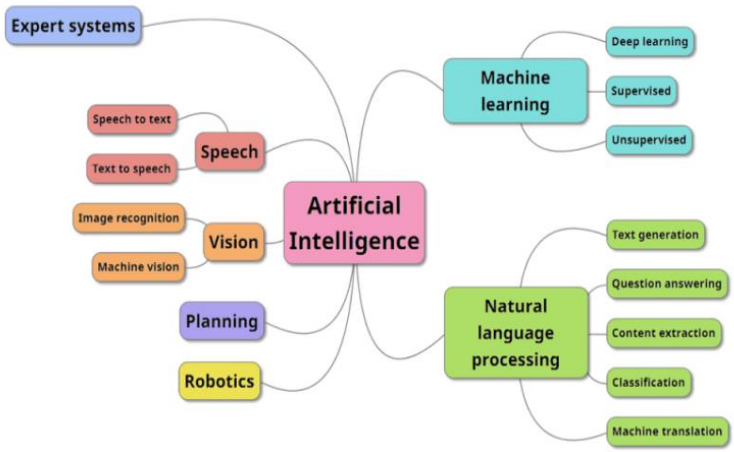

Figure 2: Types and Uses of AI
(Source: [7]

The authors discussed the importance of AI in the detection and prevention of malware due to the recognition of intricate patterns which normally measure neutral things. The study also introduces AI as an innovative answer that can detect the threat in real-time, since machine learning models using enormous data can be trained to do so. The role of AI incorporates preprocessing of data, deriving a feature set, training a model and providing a high accuracy of threat classification [7]. The architecture is adaptive to learning to enable systems to constantly change with new malware versions. The findings of the study AI play a crucial role in facilitating intelligent and automatised options for cybersecurity, which is critical to the digital world. ***[Refer to Figure 2]***

The authors concentrated on the use of the AI approach to enhance the precision and effectiveness in the identification and categorisation of malware. The authors create AI models capable of analysing behavioural features and code structure of malicious programs instead of using a signature-based type of detection [8]. The study points out the necessity of selecting the features and training on various datasets to decrease false positives. It concludes that AI not only provide the advantages of threat identification but is also capable of accelerating the process of classification, thus, it can be of critical importance used in proactive cybersecurity defence systems.

C. Implementation Barriers and Ethical Considerations

The authors critically discuss the implementation problems of AI in smart healthcare systems and especially in clinical settings. Among the critical limitations of AI, the authors note the importance of data privacy issues, model instability, absence of generalizability to various patient groups. These challenges pose a serious challenge to implementation and particularly in high-risk environments where making mistakes can be fatal [9]. The research likewise touches upon the lack of uniformity in the AI models and on the impossibility of their smooth connection to the existing healthcare infrastructure. On the whole, it points to the necessity of efficient control systems, moral codes to achieve safe, clear, and dependable application of AI.

Many ethical issues are present that arise due to inequity related to AI algorithms in healthcare, especially the ones created through imbalanced and non-representative training data. They believe that this kind of prejudice and discrimination can incorrectly diagnose or make treatment suggestions to patients, affecting them out of proportion. They emphasise that the inability to deactivate the bias of datasets in AI systems can disrupt the laws of fairness and reliability in AI systems. One possible measure to address this problem, that is, managed data sharing between institutions in order to increase the quality and breadth of datasets, is proposed by the study [10]. This would support the development of fairer AI and minimise the possibility of algorithmic discrimination in medical care.

III. METHODOLOGY

A. Research Design

This study focuses on an *explanatory research design* because of the study objectives that aim at examining how AI improves malware detection in connected medical equipment. It intends to describe the correlations among the AI algorithms, cybersecurity threats, and healthcare performance. This design helps in understanding the role of AI in the development of secure and adaptive solutions in the context of medical device ecosystems.

B. Data Collection and Analysis

The study is based on secondary qualitative and quantitative data methods to rely on. Gaining an

understanding of how AI could be used in the real-world environment and what issues are concerned with cybersecurity, qualitative data provides case studies, journals, articles, and healthcare industry reports. Quantitative data involves graphs, charts, and other performance levels describing the accuracy of detection, the false-positive rates, and the efficiency of the systems with the help of AI. Combined, these techniques will help conduct a thorough investigation of the success of AI in the protection of connected healthcare tools.

C. Case Studies/Examples

Case Study 1: Medtronic Cardiac Devices Cyber Vulnerability

During 2019, the implantable cardiac devices of Medtronic, such as pacemakers and defibrillators, were identified vulnerabilities because of an unsecured wireless communication protocol. There is a possibility that hackers might change settings on the devices remotely without permission [11]. This seriously questioned the safety of patients and data protection. The event compelled the corporation and the regulatory agencies to embark on high-level security systems, such as the employment of AI-operated intrusion detection systems. AI was suggested in order to track abnormal data traffic, raise the alerts on abnormalities and be able to provide immediate responses to possible cyberattacks on the connected medical systems.

Case Study 2: Johnson & Johnson Insulin Pump Alert

In 2016, Johnson & Johnson warned of a security flaw in its OneTouch Ping insulin pump, and this device communicated unencrypted via wireless. A hacker in range might as well be able to administer illegal amounts of insulin. No actual attacks were reported. However, the case showed the danger of hacked wireless medical equipment [12]. The case prompted the medical sector to explore the application of AI in tracking the use patterns, recognising abnormal dose-taking habits, and detecting unauthorised orders to stop possible misuse and protect patient well-being.

Case Study 3: NHS Smart Healthcare System Trials

The NHS of the UK introduced the smart healthcare trials by blending the hospital networks with the connected devices to monitor patients in real-time. Application of AI algorithms During tests, ready-made AI algorithms were used to detect the presence of malware activity in the system of connected medical devices [13]. These machine learning tools taught themselves to detect unusual traffic or malicious login attempts by learning the regular behaviours of the device. The experiment and trials proved that the AI technology might facilitate a massive decrease in cybersecurity risks and preserve device functions and the condition of patients.

D. Metrics of Evaluation

AI-based malware detection success will be assessed with the *key cybersecurity metrics* such as the detection rate, false-positive rate, reaction time, and system adaptability. Other measures are the *accuracy of models*, *malware classification quality*, and the effect on patient *security and safety and data protection*. Such measures will facilitate an evaluation of AI solution effectiveness in actual health care conditions and form the basis of future advances in cybersecurity design of connected medical devices.

IV. RESULTS

A. Data Interpretation

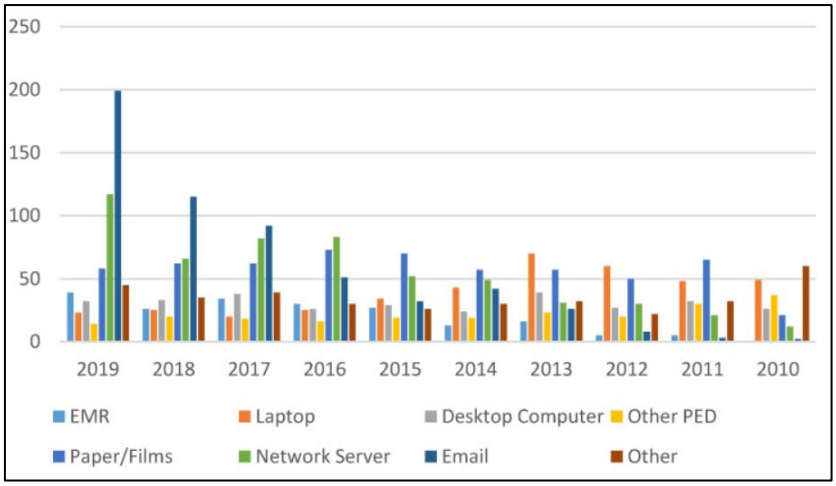

Figure 3: Healthcare Data Breach Incidents
(Source: [14])

Figure 3 demonstrates the amount of healthcare data breach events between the years 2010 and 2019. In 2019, the prevalence of EMR (Electronic Medical Records) increased to nearly 200 breaches, then the Network Servers has 120. Between 2016 and 2018, the number of breaches was high on EMR, Network Servers, and Paper/Film has more than 60 per year [14]. The number of incidences by Laptops, Desktop Computers,

and Other PEDs (Portable Electronic Devices) was moderate yet steady across all the years. The data spots a considerable increase in the number of breaches to the digital platforms, particularly after 2015, indicating that there is an elevated danger of cybersecurity threats in healthcare IT.

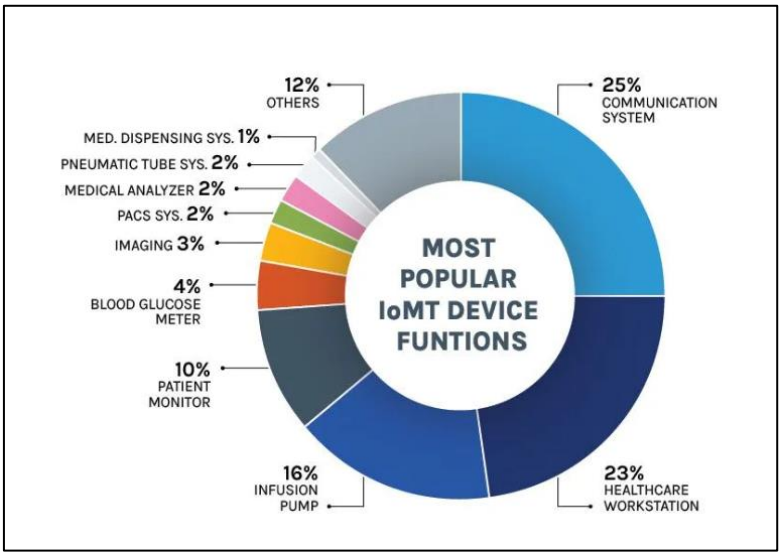

Figure 4: Most Popular IoMT Devices Functions
(Source: [15])

The most well-liked IoMT (Internet of Medical Things) device capabilities appear in the picture. Communication systems have 25% and healthcare workstations has 23% take the leading positions, but are not related to patients directly [15]. The 25% combined consists of the patient-connected devices such as infusion pumps which has 16% and patient monitor 10% [15]. The rest 25% is split amongst other options of systems such as blood glucose by 4%, imaging 3%, PACS 2%, medical analysers 2%, pneumatic tube systems 2%, and others 12% [15]. The devices facilitate important healthcare processes including emergency communication, data storage, diagnostics, and dispensing (medication), which shows their significance in the contemporary healthcare infrastructure.

B. Findings

The findings shows that there has been a high-level growth of healthcare data breaches although the number rocketed after 2015. In 2019 alone surpassed 200 on number of EMR breaches and 120 on Network Server breaches [14]. Between 2016 and 2018, the number of breaches exceeded 60 cases at the level of EMRs, network systems, and paper records annually [14]. On the other hand, 25% of IoMT devices are communication systems, 16% are infusion pumps, and 10% are patient monitors, which are the essential tools of contemporary care [15]. These devices are a necessity and at the same time a very exposed part of the digital networking. The alarming malware attacks and the increasing dependence on the IoMT prove that AI-based malware recognition is much needed to safeguard unbarred structures and guarantee good care services.

C. Case Study Outcomes

Table 1: Case Study Outcomes

Case Study	Key Findings	Relevance
Case Study 1: Medtronic Cardiac Devices	Devices were vulnerable to remote hacking via unsecured wireless links [11].	Shows AI's role in detecting abnormal data traffic and enhancing device security.
Case Study 2: Johnson & Johnson Insulin Pump	The wireless pump risked unauthorised insulin delivery due to no encryption [12].	Emphasises AI's value in monitoring usage patterns and preventing misuse.
Case Study 3: NHS Smart Healthcare Trials	AI detected malware by learning device behaviour in real-time [13].	Validates AI as a scalable, proactive cybersecurity tool in hospitals.

(Source: Self-developed)

Table 1 highlights the case study outcomes of three different case studies related to the topic. The real-world case studies highlight how AI identify and addresses the issues of cybersecurity in medical devices. The key findings and relevance enhance the device protection in healthcare.

D. Comparative Analysis

Table 2: Comparative Analysis

Author	Focus Area	Key Findings	Limitations
[5]	Cybersecurity in IMDs	IMDs are highly vulnerable due to weak encryption and poor authentication [5].	Lacks technical solutions; focuses on general risks.
[6]	Medical device security lifecycle	Recommends risk-based security across device lifecycle stages [6].	No direct focus on AI or real-world application.
[7]	AI for malware detection	AI enables real-time, adaptive malware detection using big data [7].	Effectiveness depends on the quality and variety of training data.
[8]	AI-based classification	AI improves malware classification by analysing behaviour and code.	Relies heavily on proper feature selection and dataset quality.
[9]	AI implementation barriers	Highlights data privacy, model instability, and poor integration [9].	Lacks specific case studies and quantifiable analysis.
[10]	Ethical bias in AI	Bias in training data leads to unfair AI decisions, promotes data sharing.	Focuses only on fairness, overlooks technical integration.

(Source: Self-developed)

Table 2 highlights the comparative analysis where different authors show their perspective regarding the topic. AI is one of the most important aspects these days, especially in the healthcare sector. The ethical and implementation barriers are also discussed through the perspective of different authors, which can highlight the data privacy and poor integration.

V. DISCUSSION

A. Interpretation of Results

The secondary data has indicated the increasing cybersecurity risks of connected medical devices because they have poor encryption as well as obsolete systems, which makes them prone to attacks. AI is argued as an efficient mean of real-time detection of malware based on their patterns and behavioural analysis [7]. According to the studies, the efforts to estimate AI capabilities must involve cooperation among stakeholders and enhanced data-sharing to establish secure, flexible, and equitable AI systems within smart healthcare settings.

On the other hand, there is an emerging cybersecurity threat in healthcare IT, especially, since 2015. More than 200 EMR breaches and 120 network server breaches were identified in the year 2019 alone, representing the shift toward the orientation of attacks on digital platforms [14]. At the same time, in healthcare operations, IoMT devices are responsible for critical business processes such as network communications equipment 25%, Infusion pumps 16%, and Patient monitors by 10% are used the most [15]. They become more connected and, thereby, expose themselves to malware, which is why using AI-powered detection systems becomes critically important to protect the healthcare infrastructure.

B. Practical Implications

The study raises the point where there is an urgent need to develop efficient AI-based malware-detection systems in the connected medical devices to reduce the cybersecurity risks. With the increasing level of EMR and IoMT integrations into patient care, their susceptibility may interfere with data and even lives [16]. Real-life implementation of AI allows detecting threats in real-time, automated prevention, and active learning, empowering healthcare IT infrastructures by empowering them to become more resilient, secure, and responsive to changing cyber threats.

C. Challenges and Limitations

The shortcoming of this secondary study is the lack of access to real-time clinical information and using published literature that might be not up-to-date to observe the current attack trends. The findings of the study cannot be generalised due the different devices that AI within deployed [17]. These limitations are setbacks to evaluating AI workability on changing healthcare situations, which reiterates the importance of real-life case studies and in-life verification of the system on security.

D. Recommendations

Healthcare facilities ought to ensure that AI-enhanced threat emanation is combined with the current IT infrastructure, which is practical in enhancing cybersecurity concerns in interconnected medical devices. The governments and producers should work together to come up with regulatory criteria that will prescribe embedded AI security in any IoMT devices. According to secondary research, hospitals ought to implement the continuous monitoring systems with different sets of training data in order to limit false positives and bias [18]. Better data sharing between organizations will also be able to enhance the training of an AI model. Regular audits, employee education, and ethical supervision of employees are suggested to guarantee a long-term resilience and patient safety.

VI. CONCLUSION AND FUTURE WORK

The research concludes that opinion consists in the AI-driven malware detection as one of the necessary steps toward the security of the connected medical devices of the healthcare sector. As the level of breach of

data increases, and more devices are susceptible to apps and software, AI has adaptive and real-time protection. Nonetheless, ethical, technical, and integration issues should be addressed to achieve the safe, trustworthy, and scalable smart healthcare environment.

The future work is to implement AI models in clinical practice by focusing on their live testing and evaluation to measure the effectiveness in real-time, false positives, and interoperability. Besides, creation of moral taxonomies, powerful databases, and inter-institutional will improve equity, visibility, and AI-performance of safeguarding patients and data within intelligent healthcare administrations.

REFERENCES

1. Jiguru, L.V., 2021. A Review of Cloud-based-Malware-Detection using Artificial Intelligence in the Cyber Domain. *Journal of Interdisciplinary Cycle Research*, *13*(8), pp.282-289.
2. Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A. and Jain, R., 2020. Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet of Things Journal*, *8*(11), pp.8707-8718.
3. Joyia, G.J., Liaqat, R.M., Farooq, A. and Rehman, S., 2017. Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain. *J. Commun.*, *12*(4), pp.240-247.
4. Pustokhina, I.V., Pustokhin, D.A., Gupta, D., Khanna, A., Shankar, K. and Nguyen, G.N., 2020. An effective training scheme for deep neural network in edge computing enabled Internet of medical things (IoMT) systems. *IEEE Access*, *8*, pp.107112-107123.
5. Tabasum, A., Safi, Z., AlKhater, W. and Shikfa, A., 2018, August. Cybersecurity issues in implanted medical devices. In *2018 International Conference on Computer and Applications (ICCA)* (pp. 1-9). IEEE.
6. Schwartz, S., Ross, A., Carmody, S., Chase, P., Coley, S.C., Connolly, J., Petrozzino, C. and Zuk, M., 2018. The evolving state of medical device cybersecurity. *Biomedical instrumentation & technology*, *52*(2), pp.103-111.
7. Faruk, M.J.H., Shahriar, H., Valero, M., Barsha, F.L., Sobhan, S., Khan, M.A., Whitman, M., Cuzzocrea, A., Lo, D., Rahman, A. and Wu, F., 2021, December. Malware detection and prevention using artificial intelligence techniques. In *2021 IEEE international conference on big data (big data)* (pp. 5369-5377). IEEE.
8. Huang, L.C., Chang, C.H. and Hwang, M.S., 2020. Research on malware detection and classification based on artificial intelligence. *International Journal of Network Security*, *22*(5), pp.717-727.
9. Nasr, M., Islam, M.M., Shehata, S., Karray, F. and Quintana, Y., 2021. Smart healthcare in the age of AI: recent advances, challenges, and future prospects. *IEEE access*, *9*, pp.145248-145270.
10. Gaonkar, B., Cook, K. and Macyszyn, L., 2020. Ethical issues arising due to bias in training AI algorithms in healthcare and data sharing as a potential solution. *The AI Ethics Journal*, *1*(1).
11. Medtronic.com, 2021, *product-security* Available at: https://www.medtronic.com/au-en/product-security.html [Accessed on: 29th November, 2022]
12. Mobihealthnews.com, 2016, *johnson-johnson-warns-insulin-pump* Available at:https://www.mobihealthnews.com/content/johnson-johnson-warns-insulin-pump-users-possible-hacking-risk [Accessed on: 29th November, 2022]
13. Healthcareitnews.com, 2022, *uk-nhs-digital-runs-wireless-tech-trials* Available at: https://www.healthcareitnews.com/news/emea/uk-nhs-digital-runs-wireless-tech-trials-improve-health-and-care-services [Accessed on: 30th November, 2022]
14. Europepmc.org, 2020, *article* Available at: https://europepmc.org/article/PMC/7349636 [Accessed on: 22nd November, 2022]
15. Forescout.com, 2022, *risk-of-connected-medical-devices* Available at: https://www.forescout.com/research-labs/risk-of-connected-medical-devices/ [Accessed on: 24th November, 2022]
16. Thanh, C.T. and Zelinka, I., 2019, December. A survey on artificial intelligence in malware as next-generation threats. In *Mendel* (Vol. 25, No. 2, pp. 27-34).
17. Ross, P.T. and Bibler Zaidi, N.L., 2019. Limited by our limitations. *Perspectives on medical education*, *8*, pp.261-264.
18. Chintale P: Optimizing data governance and privacy in Fintech: leveraging Microsoft Azure hybrid cloud solutions. Int J Innov Eng Res. 2022, 11:
19. Goli, S. R., & Goli, A. K. R. (2022). Strengthening Data Governance and Privacy: Utilizing Amazon AWS Cloud Solutions for Optimal Results. Available at SSRN 5317148.
20. Goli, Arun Kumar Reddy. "DEVOPS METRICS THAT MATTER: BUSINESS IMPACT OF DORA AND SRE RELIABILITY INDICATORS."
21. Konda, R. End-to-End Observability in API-Driven Architecture using MuleSoft and Prometheus.