Journal of Rare Cardiovascular Diseases
ISSN: 2299-3711 (Print) | e-ISSN: 2300-5505 (Online)
www.jrcd.eu
RESEARCH ARTICLE

Development of Cyber Strategy to Secure Medical Device from Digital Hacking

Dr. Omkar Sunil Sonawane
Assistant Professor, Department of Defense and Strategic Studies, Savitribai Phule Pune University, India

*Corresponding Author

Article History
Received: 02.10.2025
Revised: 22.10.2025
Accepted: 20.11.2025
Published: 30.11.2025

Abstract: As revolution in the field of IT has enabled unending technological innovations, it has also brought up several security challenges pertaining to newer asset i.e. information. Therefore, protecting these assets of information has become an equally important task and any negligence towards it, can turn out to be fatal. Information security, as suggested is about seeking IT security and securing information. There is a very thin line between data and information. Data is distinct pieces of information, which is formatted in unique ways and patterns. Recently, medical data and devices' hacking incidences are noted globally. Hackers hack medical devices and medical dataset to get the access of sensitive information. To avoid the software driven data manipulation in the event of digital hacking, proposed study presents the strategy based on the hypothetical analysis for securing the healthcare devices and data.

Keywords: **Cyber warfare, cyber security, medical device hacking, data protection**

INTRODUCTION

With advances in digitalization of cardiac implantable electronic technologies, patients have greater opportunities for improved autonomy, quality of life, and possible increase in life expectancy. Information technology has improved the coordination between mobile apps, medical devices, and the healthcare provider or electronic medical database for both the delivery and exchange of needed medical data or information. [1]

Think of imaging, patient monitoring, or surgery equipment. A key measure to secure any networked device from attacks is to regularly provide software updates to address vulnerabilities. However, it has been repeatedly reported that a plethora of connected medical devices remain outdated and vulnerable. The prevalence and risks of unpatched and outdated medical devices have been raised by governmental actors such as the FBI, industry reports, and academic studies. [2]

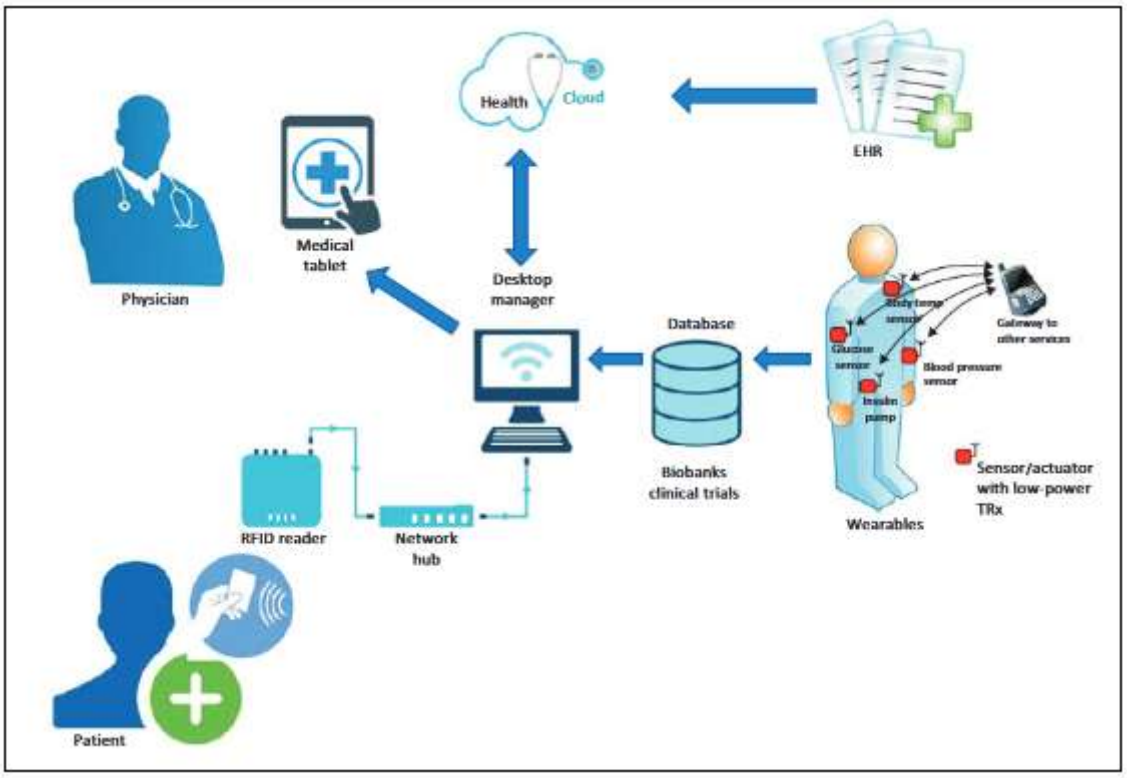

Fig.1: Representation of Internet of Things devices in healthcare [3]

The rising cost of care and resource limitations within the medical industry led to the embracement of technological advancements, the most notable of which is the use of Internet of Things (IoT) devices. The IoT devices in healthcare enable real-time data collection, analysis and sharing of data with other devices and the cloud aiding in remote patient monitoring and emergency response services. These devices transmit data via wireless networks such as Wi-Fi, LoRa and Bluetooth within a hospital network facilitating data integration to provide better treatment. (Refer Fig.1 above) [3]

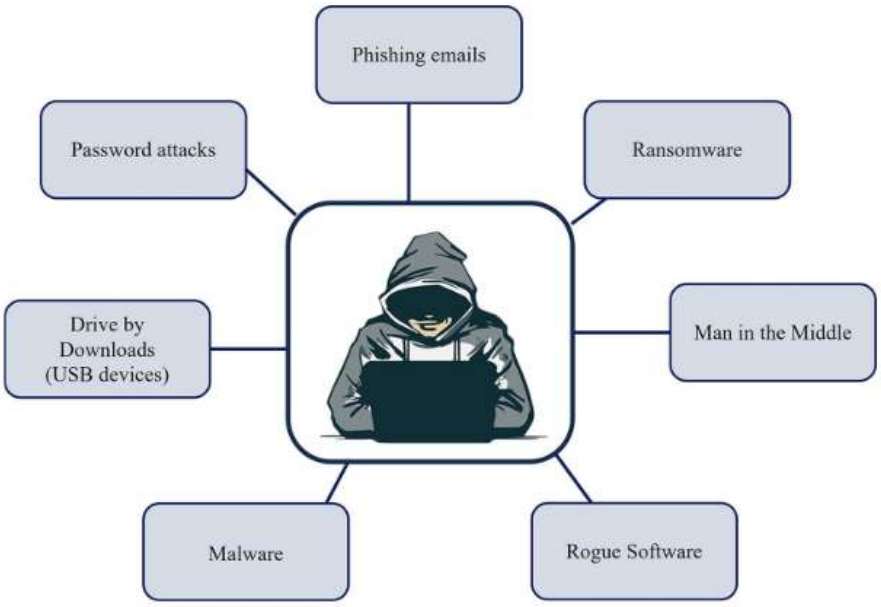

Fig. 2: Methods hackers utilize for infiltrating medical devices [4]

The wireless transfer of information requires interfaces that come also with inherent security risks. Since most devices contain proprietary communication protocols that do not allow direct access to the internet, they connect instead to the internet via a secondary device, such as a bedside monitor or a mobile device. A single error in the implementation of security protocol or access vulnerability could allow for an unchecked code to run and permit the opening or modification of the entire cyber system. Thus, through a single weak entry point, a cyber breach has the potential to affect both the health care institution and the individual patient. [4,5]

2. Literature Review

Cyber security doctors must continuously analyze volumes of data from devices, networks, operating systems and applications to detect abnormalities and vulnerabilities. This requires sharp critical thinking skills to parse through noise and pinpoint anomalies indicative of emerging risks, such as unusual traffic patterns or firmware irregularities. Strong logic and deductive reasoning allows insightful extrapolation from identified issues to assess downstream impacts across wider systems. [6]

Data security methods are used by organizations to protect data from cyber attacks, data breaches and data losses. Data privacy is related to access of personal information by authorized people plus organizations and simultaneously the person retains control over it [3]. The main challenges of data security in healthcare sector are security of mobiles plus data stored in them, computers and medical devices, software updates, remotely scanning all devices for anti-viruses, phishing attacks and data breaches. The main challenges of data privacy in healthcare sector are legislative gaps, absence of trust due to lack of privacy and patients don't have control over shared medical records. [7]

Cyber Security, on the other hand is the practice of safeguarding digtial assets from potential data breaches and protects it from any unauthorized access. It is the subset of information security that deals with security of IT and cyber space. It is the practice of safeguarding confidential information and protect systems of information from any unauthorized access by implementing security procedures, protocols and technology, in order to mitigate potential cyber threats, which can be both; online and offline. The whole idea behind cyber security is to mitigate cyber threats of businesses, enterprises, governments, organizations, military and individuals in general. Its key role is to protect information from unauthorized access. It is the practice, to safeguard one's valuable data in its electronic format. [8,9]

These new cyber spaces are increasingly being used by humans to make their life more meaningful, simple, comfortable and productive enough without having to face much physical difficultly or stress. It has become so integrated in our daily lives that sometimes its adverse effects are not taken into consideration. Individuals now resort to cyber space for sending a text message or an email to a colleague, downloading or uploading digital files, listening to music, access to

information through the world wide web using search engines, making online purchases, managing online bank account, public distribution systems, online voting, lottery, dating, chatting, virtual meeting, etc. [10,11]
Cybercrime encompassed almost every areas of society and has affected people of all ages in many different ways leaving victims helpless, worried and vulnerable. It is increasing at a very fast rate as compared to traditional crime, which is now estimated to be in billions. Due to this nature of cybercrime, anyone can be a victim to it, which could be anyone from, a young woman who is harassed and bullied online to a senior citizen, who has been scammed for money through an false online retirement pension scheme. [12-14]
Cyber warfare is use of computer technology by a nation state in order to direct or redirect cyber-attack against a nation state, which can potentially harm or destroy computers, networks and satellites, which coordinate military systems. Such attacks are a matter of concern, especially in the areas of command and control system, defence networks, weapons system, and guided missile systems, which require command, control and computer to operate. The impact of cyber warfare upon national security is such that all the government intuitions and organizations require collaborative efforts to counter these cyber threats and challenges. [15,16].

METHODOLOGY & MATERIALS

3. Research Methodology

The research work largely relies on historical analytical approach to help researcher to make use of observations based on the events of past and current. The research adopts an integrated perspective on dynamically advancing cyberspace and challenges its poses and attempts to combine insights from different disciplines such as science and technology, political science, strategic studies as well as from organisational change to understand the macro and micro aspects of research which often remain under-explored.
The research draws upon the results of other research work as well as primary analysis literary to find an answer to research questions. The research also delves on insights from experts who are working the field of cyber security that predominantly includes state and non-state institutions either fully or partially funded by state. The main aim of this research work is to apply the method of introspective thinking to India's national security with a reference to cyber security by the means of discovery through current events, trends, facts, data, observations, perceptions and attitudes.
The research adopts a holistic approach in exploring the research question and goes beyond traditional approach of mere collection of data and facts. Instead, it focuses on deepening the insights, analysis, evaluation and interpretation of primary data as well as secondary data, which are the integral parts of the research model. This research undertakes a critical evaluation and interpretation of pertinent data, documents, records, reports, and events in such a manner that general laws and trends can be framed.
To use secondary data for the research, the researcher has depended on secondary literature such as magazines, newspaper, reports, research papers, research journal, websites, government data, government websites, policies, non-profit agency reports, statistical data, monthly, yearly, report of leading think tanks and institutions, report of international bodies and organizations, international treaties and agreements, audio – video content, documentaries, and information from other media sources like blogs and web pages. The research is built around the instances and developments that is crucial to cyberspace and technologically enabled spaces that generate data of individuals. In addition, it also investigates into a regulatory framework that governs the complex space driven by internet and technology.
Following hypotheses has been tested for sample size of 300 participants:

H0: There is no need of the counter measures for medical data and device security.
H1: There is a need of the counter measures for medical data and device security.
H0: Digital data hacking cannot be a national threat.
H1: Digital data hacking can be a national threat.

For hypothesis testing is conducted by using the IBM-SPSS software and results are interpreted in the next Section-4 of this paper.

RESULTS AND DISCUSSION

H0: There is no need of the counter measures for medical data and device security.

H1: There is a need of the counter measures for medical data and device security.

		Counter measures	Medical data and device security
Counter measures	Pearson Correlation Sig. (1-tailed) N	1 300	0.902 0.002 300
Medical data and device security	Pearson Correlation Sig. (1-tailed) N	0.902 0.002 300	1 300

*Correlation is significant at 0.05 levels (1-tailed)

Correlation of Counter measures with itself (r=1) and the number of non-missing observations for height (n=300). The Correlation between Counter measures and Medical data and device security (r=0.902) is based on n=300 observations with pair wise non-missing values. Correlation of Medical data and device security with itself (r=1) and the number of non-missing observations for weight (n=300). Counter measures and Medical data and device security have a statistically significant linear relationship (r=0.902, $p < 0.05$). The direction of the relationship is positive, i.e., Counter measures and Medical data and device security are positively correlated. Hence, the positive hypothesis is accepted.

H0: Digital data hacking cannot be a national threat.

H1: Digital data hacking can be a national threat.

		Digital data hacking	National threat
Digital data hacking	Pearson Correlation Sig. (1-tailed) N	1 300	0.811 0.001 300
National threat	Pearson Correlation Sig. (1-tailed) N	0.811 0.001 300	1 300

*Correlation is significant at 0.05 levels (1-tailed)

Correlation of Digital data hacking with itself (r=1) and the number of non-missing observations for height (n=300). The Correlation between Digital data hacking and National threat (r=0.811) is based on n=300 observations with pair wise non-missing values. Correlation of National threat with itself (r=1) and the number of non-missing observations for weight (n=300). Digital data hacking and National threat have a statistically significant linear relationship (r=0.811, $p < 0.05$). The direction of the relationship is positive, i.e., Digital data hacking and National threat are positively correlated. Hence, the positive hypothesis is accepted.

According to the hypothesis testing by statistical analysis we recommend the following counter measures:

Counter Measures for Denial of Service Attack:

- Install robust IT systems and an intrusion detection system, which can detect DoS attack.
- Block and ban IP addresses, which are potentially malicious and responsible for earlier attacks in order to avoid incidents in future.
- Add necessary measures and safety mechanism for UPD and ICMP traffic.
- Reject data packets coming from unknown IP addresses.
- Implement strict password protocol and rename administrator's account as and when necessary.
- System should have effective firewall setting to deal with DoS attacks.
- System should remain offline when the machine is not in use.
- System should have anti-virus installed and keep it up to date.

Counter Measures to control Social Engineering Attack:

- Have a good and effective awareness and training programme, detailing the various social engineering techniques.
- Conduct awareness campaigns and put up posters and warnings as constant reminders.

Countermeasures to prevent medical device hacking:

- Focus on access controls, network isolation, and proactive maintenance.
- Implement multi-factor authentication (MFA) to restrict device access to authorized personnel only.
- Regularly review and update permissions to minimize unauthorized entry risks.
- Network and Software Protections.
- Conduct vulnerability scans with penetration testing.
- Encrypt data at rest and in transit using strong protocols, while minimizing collected data.
- Deploy real-time threat monitoring with AI tools for swift detection and response.
- Train staff on phishing recognition, cyber security awareness, and safe device handling to build a human firewall.

It is necessary to incorporate the above suggested counter measures to maintain the social and economical security.

CONCLUSION

As discussed in this paper, medical data and devices hacking can be a national threat and hence, counter measures need to be practices. In order to counter the threat of cybercrime, cyber terrorism and cyber warfare, there is a need for a cyber security incident response mechanism, which should consist of five key stages. These stages include detection, identification and defence against the attack, design and deploying counter measure and lastly post conflict investigation and recovery. As a future study, it is necessary to conduct cyber attack awareness training for corporate and citizens to lower the risk of digital hacking.

REFERENCES

[1] Owolabi, Babatunde O. "Cyber-physical security in smart healthcare: protecting IoT-enabled medical devices from spyware, ransomware, and network-based exploits." Int J Res Publ Rev 6.3 (2025): 1812-26.

[2] Kustosch, Lorenz, et al. "Patching Up: Stakeholder Experiences of Security Updates for Connected Medical Devices." 34th USENIX Security Symposium (USENIX Security 25). 2025.

[3] Khan, Na-ella, and Riaan J. Rudman. "IoT medical device risks: Data security, privacy, confidentiality and compliance with HIPAA and COBIT 2019." South African Journal of Business Management 56.1 (2025): 4796.

[4] Torgersen, Leanne NS, et al. "Patient informed consent, ethical and legal considerations in the context of digital vulnerability with smart, cardiac implantable electronic devices." PLOS digital health 3.5 (2024): e0000507.

[5] Al-Juboori, Shaymaa, and Suliat Jimoh. "Cyber-securing medical devices using machine learning: A case study of pacemaker." Journal of Informatics and Web Engineering 3.3 (2024): 271.

[6] George, A. Shaji, and AS Hovan George. "Safeguarding the Cyborg: the emerging role of cybersecurity doctors in protecting human-implantable devices." Partners Universal International Research Journal 2.4 (2023): 1-12.

[7] Brass, Irina, et al. "Emerging Digital Technologies in Patient Care: Dealing with connected, intelligent medical device vulnerabilities and failures in the healthcare sector." Workshop Report: PETRAS National Centre of Excellence in IoT Systems Cybersecurity. PETRSA & bsi, 2023.

[8] Kamalov, Firuz, et al. "Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective." Sustainability 15.4 (2023): 3317.

[9] Khan, Abdullah Ayub, et al. "Data security in healthcare industrial internet of things with blockchain." IEEE Sensors Journal 23.20 (2023): 25144-25151.

[10] Mohamed, Nachaat, et al. "Understanding the threat posed by Chinese cyber warfare units." 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA). IEEE, 2023.

[11] Digmelashvili, Temur. "The impact of cyberwarfare on the national security." Future Human Image 19 (2023): 12-19.

[12] Swallow, Robert Chandler. "Considering the cost of cyber warfare: advancing cyber warfare analytics to better assess tradeoffs in system destruction warfare." The Journal of Defense Modeling and Simulation 20.1 (2023): 3-37.

[13] Khan, Muhammad Younis. "Cyber security: Recent cyber-attacks as a challenge to national economic security." International Journal of Modern Sciences and Multidisciplinary Studies (IJMSMS) 2.01 (2023): 72-100.

[14] Mohammed, Anwar. "Protecting Space Assets: Cybersecurity Challenges and Solutions for the Final Frontier." Baltic Journal of Engineering and Technology 2.1 (2023): 55-61.

[15] Zwilling, Moti, et al. "Cyber security awareness, knowledge and behavior: A comparative study." Journal of Computer Information Systems 62.1 (2022): 82-97.

[16] White, Garry. "Generation Z: Cyber-attack awareness training effectiveness." Journal of Computer Information Systems 62.3 (2022): 560-571.