Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2021.015351
Article

Tech Science Press

Healthcare Device Security: Insights and Implications

Wajdi Alhakami[1], Abdullah Baz[2], Hosam Alhakami[3], Masood Ahmad[4] and Raees Ahmad Khan[4,*]

[1]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif P.O. Box 11099, Taif, 21944, Saudi Arabia
[2]Department of Computer Engineering, College of Computer and Information Systems, Umm Al-Qura University, Makkah, 21955, Saudi Arabia
[3]Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah, 21955, Saudi Arabia
[4]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow-226025, Uttar Pradesh, India
[*]Corresponding Author: Raees Ahmad Khan. Email: khanraees@yahoo.com
Received: 17 November 2020; Accepted: 08 December 2020

Abstract: Healthcare devices play an essential role in tracking and managing patient's safety. However, the complexities of healthcare devices often remain ambiguous due to hardware, software, or the interoperable healthcare system problems. There are essentially two critical factors for targeting healthcare: First, healthcare data is the most valuable entity on the dark web; and the second, it is the easiest to hack. Data pilferage has become a major hazard for healthcare organizations as the hackers now demand ransom and threaten to disclose the sensitive data if not paid within the stipulated timeline. The present study enlists a thorough research on the data violation cases and the possibilities of data infringements likely to happen in the next five years. This paper discusses about the healthcare device, security of healthcare and year wise security flaws. Healthcare data breaches analysis and forecasting of data breaches and causes of breaches also discussed. Open research challenges and future directions for healthcare industries also discussed.

Keywords: Healthcare devices; device security; healthcare device hijack; hardware; software and network security

1 Introduction

As per the very recent article published by Forbes magazine on 24th March 2020, when the entire world was fighting with COVID-19 and all the research labs were busy in developing a vaccine for this pandemic, then the attackers hit on a vaccine testing center (*Hammersmith Medicines Research*) and stole the data [1]. The hackers also issued a warning to publish the data online if their ransom demand was not complied within a specified timeline. However, in the midst of the present humanitarian crisis of COVID-19, there has been an agreement between the attackers and the healthcare sector about not invading the healthcare data. In the wake of the alarmingly growing episodes of healthcare data pilfering, this study is dedicated to examine the issues and challenges pertaining to the security of the healthcare devices. Computational and transmission tasks are

performed on the healthcare devices with the help of software. Software of healthcare devices should fulfill system properties, like safety, security, reliability, etc. According to an analytical report issued by the Food and Drug Administration (FDA), it observes that 20 to 25% of the vulnerabilities arise due to the software of the healthcare devices. Recently FDA's chief scientist declared that even a slight change in the security of a healthcare device can be life threatening for the patients [1–3].

Mostly implantable, wearable and onsite healthcare devices regulator by the controlling message programs over the network. Healthcare device and controlled device send messages to each other than the attackers trespass over the networks. Most of the implantable and wearable devices have no encryption, authentication and integrity checking mechanism so these networked devices easily come under the attackers attacks [2,3].

FDA's Safety Commutation has identified *URGENT/11* vulnerabilities that arise by the use of the third party software component. These vulnerabilities can retard the efficacy of the healthcare device. URGENT/11 vulnerabilities can make a healthcare device a hub of criminal activity and change the functions of the device through the Denial of Services (DoS) attack. URGENT/11 is found in IPnet, which is the third party software component that helps the networks to communicate with other computers. Though some of the reputed vendors do not support the IPnet, some vendors allow the use of IPnet without support [4]. For this reason, the FDA has issued guidelines to sensitize the manufacturers who develop the healthcare devices and the patients who buy those [5].

Generally, publicly available software tools improve the quality of data available for health professionals and users. Healthcare devices must be enabled by high quality software only because the inaccurate outputs can harm the patients' life. Moreover, it is imperative for the developers to religiously adhere to the stipulations of FDA because in case of any aberrations in the device, the developers are the first to be questioned [6]. A relevant example in this context is the cyber-attack on a hospital in Washington DC in 2016. The hackers hijacked the systems and disabled the digital healthcare services of the hospital for three days. Most of the data breaches are initiated by MEDJACK attacks or healthcare device hijack.

Security challenges continue to beset the software based healthcare devices because the developers cannot identify the possible vulnerabilities at the time of the development of software. However, the hackers can easily trace these susceptibilities in the devices [7–10]. It is imperative for the developers to ensure that the devices are resistant to all malicious invasions and the patients are assured of safe and accurate data at all times through their device. Malicious attacks on hardware, software and interoperability are mostly done on networked connected devices and this is likely to increase to 25 million in 2020 [8]. We are considering here the overall security of healthcare devices. Hardware and communication of the healthcare devices is controlled by the software or operated by the software. Hazards in healthcare devices can arise any time like accidental failure, software error, and network failure and cybersecurity risk [9].

The contributions of this research endeavor are as follows: Section 2 of this paper discusses the security of healthcare devices and its components. Section 3 details the history of the healthcare device and problems associated with them. Healthcare data breach analysis has been discussed in Section 4. Security challenges have been discussed in Section 5. Healthcare device cost analysis and maintenance cost forecasting has been done in Section 6. Our study has predicted the settlement cost and the maintenance cost because the cost is directly dependent on the economic feasibility of the healthcare. Discussion and forecasting data comparisons results analysis has been described in Section 7. Section 8 concludes this study.

2 Healthcare Devices and Security

A Healthcare device is a combination of hardware and software. These are important issues from the perspective of security. The World Health Organization (WHO) defines healthcare devices as, "*a machine*

which is used in diagnosis, monitoring, and treatment of disease". Some devices contain software, hardware, and interfaces; these are valuable terms of device's security. Healthcare devices hijack or MEDJACK is not easy because of old operating systems and minimum defense software. However, the old software can enable the carrier to hide the vulnerabilities that infect the other devices connected to each other.

The security of the healthcare device is a critical issue because the device processes any communication by running software on a specific hardware and by controlling the sensors. Major security threats happen when the devices sense wrong values because if the device reads an erroneous value, it will perform the wrong action. Malicious and unintentional changing of data can affect the safety in critical stages, thus endangering the patient's treatment. FDA classifies the healthcare device safety in three categories of high, medium, and low risk. Devices like Smartphones, Hospital PCs are also facing security issues but these devices are not considered as healthcare devices by WHO and FDA. Nearly 78% of the healthcare devices are unsecured [10–15]. Moreover, once a device is hacked, it may open the whole network of data breaches and hacks. Security precautions should be taken at the time of design and development of a device which controls the attackers from managing and implanting malicious components in the device.

The main reason for increasing data breach instances could also be attributed to the lack of requisite expertise and skilled professionals who can design mechanisms to contain malicious invasions. In addition, it is a huge challenge for the existing 7000 healthcare device manufacturers to find highly trained security practitioners. Already, nearly 80% of the manufacturers have less than 50 workers [16–21]. Hence to control the menace of cybersecurity threats, there is an imminent need to introduce apt guidelines and provide the necessary assistance to these manufactures. This will enable the manufacturers to improve the security and facilities for the patients through the mobile healthcare apps. Such types of apps provide access to useful health related data. These apps can be used for multiple purposes. This app can display, store, analyze, and transmit the data. Even though not all apps can be attacked by the attackers, precautions should be taken at the time of transmission of data.

3 Components of Healthcare Device

Any healthcare device requires few important components which makes the healthcare device useful. Without these three components, a healthcare device is like a box. Hardware is the most important component of the device [22–25]. In simple terms, the whole body of the device is the hardware. Hardware parts include the storage, scanning parts etc. Software plays an equally vital role in the utility of the device. It provides an interface between all the components in the device and user. Without application, the software device cannot be operated by the user. Internal parts of healthcare devices are connected with each other through a network. The device itself is connected to the Internet for sharing data and communicating with other devices and this is called network. Fig. 1 below illustrates the three main components of a healthcare device.

3.1 Software

Software plays an important role in the functioning and the usability of healthcare devices. Without software, healthcare devices cannot perform the task and process on the data. As much as the software is useful for the device, it is also harmful [26–29]. The computational power of the healthcare device makes the device vulnerable. Bugs or flaws in software are used by hackers to control the device or network. Software vulnerabilities are exploited by the attackers to trespass on the device through the loop whole of software. Each device's software is developed for a specific task. To sensitise the users and the developers, FDA has already identified those operating systems that are affected by the vulnerable IPnet. Some of the manufacturers also keep their customers informed about the devices that are affected by the URGENT/11, like healthcare imaging devices, an infusion pump, and anaesthesia machine [4]. In the US,

if any company wants to market its healthcare device, it is mandatory for the company to register the product with the FDA. FDA provides the guidelines for the developers to develop the healthcare device software [5,29–30]. FDA has documented four guidelines to develop software of a healthcare device-:

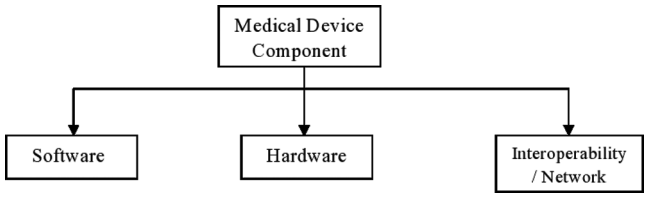

Figure 1: Components of healthcare device

1. Premarket Submissions
2. Off-The-Shelf Software
3. General Principle of Software Validation
4. Mobile Marketing Association (MMA)

All these steps are checked by the organizations before marketing their healthcare devices. A variety of software tools is available which can improve the quality of diagnosis and treatment. Affected software may harm the device and the health of the patients. FDA hopes that more devices that have the vulnerabilities related to the genuine IPnet Software will be identified soon to help the manufacturers of healthcare devices. IEC62304 is the standard of healthcare device software development. IEC62304 provides the guidelines for software development lifecycle and classification of software safety of healthcare devices.

Since most of the devices are controlled by the software, even a minor flaw or a malfunction can be detrimental to the patient's treatment. Healthcare device software safety classification has been segregated by IEC62304 in three classes: Class A; Class B; and Class C [11]. In Class-A, failure of software poses no danger to the patient's life. This type of software is inbuilt in the device, more like a general PC which stores the patients' and employees' data. In Class-B, failure of software or any error of the software does not create any serious injury to the patient. This type of software control device comes under the performance measuring the device. In Class-C, failure of software may be life threatening. These high risk types of devices software usually monitor the implantable devices which are controlled by software. Functionality of software may change the working and behavior of the healthcare device, so adhering to the software safety classification must be prioritised. Healthcare device software developers must follow the FDA guidelines for developing the software for making the software more secure and safe.

3.2 Hardware

Hardware of the healthcare device is the cabinet body and internal microcontroller chips. Micro controllers become programmable chips. Attackers can MEDJACK the device by hiding the malicious circuit for stealthy attack vectors. Attackers can perform different types of attack or MEDJACK on devices like backdoor login, password access, and wrong configuration. Hardware of healthcare devices is also important for ensuring the confidentiality of the software. Malicious hardware can be planted in the device or through the other communicating device. For instance, the web server attacker can install malicious hardware because healthcare data is stored in the web server. This type of hardware tampering can lead to faulty diagnosis and treatment, thus risking the patient's life. Moreover, maintaining consistent security of the hardware of IoT based controlled devices like CT-Scan, MRI machine, Insulin Pump, etc., is even more imperative because such devices are usually associated with the treatment of chronic diseases.

These devices also contain more sensitive hardware parts like thermal scanner, body scanner and camera. Camera and scanner are extremely vulnerable targets because the attackers can install the malicious part on the camera and scanner. The invasion takes over the control of the device and the reported data would either be corrupted by noise or get distorted. The designing phase of hardware is more time consuming because it involves the complex processes of material selection. After designing the hardware, testing is yet another time taking process. It may take one week to test a given hardware. If the tested device fails in the performance or in testing, then the hardware engineers go back to the drawing board to improvise upon the same processes. Only the thoroughly scrutinised device design which complies with the set standards of efficacy and high end performance goes to the next phase of hardware development. Hardware and software are two sides of the same coin in the healthcare device.

3.3 Interoperability

Security issues can also occur because of wireless communication over the network, unauthorized access of the patient's data, trespassing over the network to poach on the patient's health records. Data is continuously travelling over the network, so attackers can infringe upon the network any time. FDA provides the guidelines for URGENT11 in context of the third party software component which can be the cause of network trespassing. URGENT/11 Vulnerabilities occur in IPnet, IPnet is a third party software communicating component which supports the communication between the two devices [4]. All these identified susceptibilities permit the intruders to gain access to the device and control it even from remote zones. Alteration in the healthcare data may misguide the doctors. Internet connected devices transfer and send the files or data to each other within the same network. In some cases the devices are connected with the Cloud stations where the patients' data are stored and the data are sent for denoise. Data is shared over the network by the devices with the Cloud for processing. At the time of data sharing also, the attackers can gain access to classified information and exploit it. Networked devices are increasing daily, because the connected devices make it easier to access, store, transfer and share the patients' health records at any given hour from any location across the globe. However, the reckless pace of cyber intrusions is wreaking havoc on digital healthcare.

4 Work Done So Far

The history of healthcare devices can be classified in four periods. The first period was more crucial and complex for healthcare devices because of a complex system and accidental failure of devices. The second period started with implantable devices. The third period started with the unauthorized access which could harm the device. The last period of the healthcare device is about the cyber threats to the security of healthcare devices. Combining all above conclusions of software controlled devices and threats of device security arises, patient data privacy also. We have discussed the healthcare device, Polymerase Chain Reaction (PCR) which is used for thermal testing of COVID-19 patients. However PCR also has its limitations, and there could be a possibility of 1% error in the results. Thus if we have tested 100 cases, then this machine automatically produces 1 erroneous result (means if we test 100 healthy persons, then this device will find one COVID-19 patient automatically). Accidental failure of the devices has been a recurrent feature right from their invention in the 1980s to present. Accidental failure is an unintentional event and could be hardware failure, software failure or the network failure. When data is travelling over the network, a sudden network error can result in the loss of the data. Software errors can also corrupt the data and abort the processing. Hardware failure can happen because of the power failure or storage device failure. All the four periods of healthcare device have been further explained below:

4.1 Period 1—Accidental Failures of Devices (1980s-Present)

Healthcare comes under the highest risk technologies in the whole world. Ironically, the advancement in healthcare is also the reason for newly developed threats on the safety and security of device. Most of the mishaps occur due to the accidental failure of healthcare devices like software failure or the hardware problem.

4.1.1 In 1985–87—Therac-25

From June 1985- January 1987, six patients took the overdose of radiation because of the defective Therac-25. The cause is yet to be identified and could have been the user's fault, untrained healthcare staff or the wrong code of the software.

4.1.2 In 2002—Network Failure of BIDMC

On November 13, 2002, a researcher accidentally flooded the data over the network of Beth Israel Deaconess Healthcare Centre (BIDMC), this is the reason of wetting for the data access of centre. Sadly, the network recovery was only based through the network. The Healthcare centre resorted to four days of paper work until the problem could be resolved. The fault occurred due to software failure which was directing the traffic on the network.

4.2 Period 2—Implantable Devices (2000-Present)

In the 21st century, there were several changes in the design of healthcare devices and the implantable healthcare devices (IMDs) were introduced in the USA. The arrival of IMDs raised the security and reliability of healthcare device. IMDs are implanted into the human body and this creates complications in the communication between devices and doctor.

4.2.1 In 2000–Implantable Cardiac Defibrillator Failure (ICD)

FDA had to recall 114,645 defective ICDs in 2005 when a 21 year old cardiac patient died to a faulty ICD. Investigations revealed that the death happened due to short circuit in the devices.

4.2.2 In 2005–HCMSS

In June 2005, a workshop on high confidence healthcare device software and systems was conducted in Philadelphia, PA. This workshop was sponsored by FDA, NIST, NSF, NSA, and NITRD. The main purpose of the workshop was to discuss issues and challenges arising in the designing, manufacturing, certification, and use of healthcare device.

4.3 Period 3–Unauthorized Parties and Healthcare Devices (2006-Present)

50% of the healthcare devices in the USA alone in 2005, the markets were operated by software. Such devices are vulnerable to unauthorized access or healthcare device hacking or hijacking.

4.3.1 In 2006–Updates of Software for Devices

In 2006, securely updating the software of devices that allowed a client to send and install updates was a challenging task. Updates of software make the devices susceptible to *man-in-the-middle* attacks because it is difficult to trace the source of the update. The updates could be through original vendors or third party vendors.

4.3.2 In 2011–Peer-Reviewed Insulin Pump Vulnerability

Vulnerabilities in the insulin pump were disclosed by the unauthorized parties in 2011. Active and passive attacks were achieved by off-the-shelf hardware. These attacks opened vulnerability in specific insulin pumps which gave permission to unauthorized parties to "*full control on the pump: Start the insulin pump, stop and resume the insulin injection, or suddenly inject an overdose of insulin*" [5,7].

4.3.3 In 2011–Peer-Reviewed Defenses against Unauthorized Access to IMDs

RF shield, a novel security mechanism, is used to prevent unauthorized access. RF shield works as a proxy server for communicating with implantable healthcare devices (IMD). RF shield stops any unknown device from communicating with the IMD by stopping all other communication in the devices.

4.3.4 2015 to 2019–Healthcare Device Hijack

Trap X detected the Healthcare Device Hijack (MEDJACK) in *2015* for the first time. Through the MEDJACK, the hackers gain access to the computer or the network server and generate the malicious outcome. By the MEDJACK, the attackers enter the device or system via backdoor entry. When the attackers are established in the backdoor, then they steal data, send the demand for the ransom, or turn off the systems or devices. After MEDJACK was detected in 2015, 4 variations of MEDJACK had been developed till 2018 [13]. Further, in 2019 Medtronic was identified and it is used to hijack the insulin pump and cardiac device [14]. In 2017, 3 variations of MEDJACK were discovered and in 2016, there were 2 variations of MEDJACK [15]. As studies observe, it is becoming increasingly difficult to detect the fatal MEDJACK [16].

4.4 Period 4–Cybersecurity of Healthcare Devices (2012-Present)

Recently, the cybersecurity experts' attention has shifted to the cybersecurity vulnerabilities of healthcare devices. In the present era, the number of networked healthcare devices have seen a tremendous increase. Internet connected devices have lots of benefits, including online monitoring and software maintenance. However, the safety of networked healthcare devices is more critical than other devices.

4.4.1 In 2012–ISPAB Board Meeting

In February 2012, the annual Board Meeting of the Information Security and Privacy Advisory Board (ISPAB) was organized in Washington, DC. In the meeting, cybersecurity and economic benefits of healthcare devices were discussed. The meeting aimed at coordinating with the agencies involved with the regulation of healthcare devices and cybersecurity.

4.4.2 In 2013–2014—FDA Issued Guidelines on Healthcare Device Cybersecurity

The FDA issued guidelines for the management of cybersecurity in healthcare devices in June 2013, and the final guidelines were issued one year later in October 2014 [17]. The FDA guidelines focus on the security of the device at the time of design and development phase of healthcare devices. These guidelines are:

- Identification of the vulnerabilities, assets, and threats in the device's primary stage.
- Assessment of the device's functionality due to the impact of threats and vulnerabilities.
- Assessment of threat and of vulnerabilities being exploited.
- Identification levels of risk and proposed mitigation strategies.
- Assessment of residual risk and acceptance criteria of the risk.

The guideline also identifies the "core functionality" of cybersecurity activities from the National Institute of Standards and Technology (NIST) cybersecurity framework.

4.4.3 In 2013–2016—Healthcare Device Security

During this time-period, the security experts were involved in securing the networked healthcare devices. Security challenges associated with the healthcare device include: Hardware failures/software errors, radio attacks, malware and vulnerability exploits, and side-channel attacks.

4.4.4 In 2016–18—FDA Complete Guidelines on Healthcare Device

In 2016, FDA again published final guidance for premarket healthcare device cybersecurity. Thereafter in October 2018, FDA published the draft of the guidelines for manufacturing of the healthcare device.

4.4.5 From 2018—Till Present- Healthcare Device Innovation Consorting (MDIC)

In September 2018, as a MDIC steering committee member, FDA supported the report developed by the MDIC. Report was about the Advancing Coordinated Vulnerability Disclosure. The main aim of the report was to encourage the police of coordination vulnerability of Disclosure to promote healthcare device security and safety.

4.4.6 In 2019—Premarket Submission Public Workshop

On 30 January 2019, FDA organized the public workshop on cybersecurity management of premarket submissions of healthcare devices. The main aim of this workshop was to discuss about the newly draft guidance of pre-submission of healthcare devices.

4.4.7 In 2019—Patient Engagement Advisory Committee

Convened on 10 September 2019 with the intent to make FDA aware about the complexity of integrating the healthcare device security risk.

4.4.8 In 2019—URGENT/11 Cybersecurity Vulnerabilities May Introduce Risk

On 1 October 2019, FDA alerted the vendors, and patients about cybersecurity and possible vulnerabilities during the device connected with the network and server migration time.

4.4.9 In 2020—Cybersecurity Vulnerabilities in Certain Healthcare

On 23 January 2020, FDA organized a meeting of healthcare, faculties and staff for spreading awareness about the healthcare system and telemetry server at risk during the monitoring.

4.4.10 In 2020—SwenyTooth Cybersecurity

On 3 March 2020, FDA again organized a meeting of patients and vendors for awareness on SwenyTooth family of cybersecurity which may have been introduced in certain types of healthcare devices.

Our study has detailed the history of the healthcare device period-wise and year wise. Specific period and year wise events clearly explain about the risk, safety and privacy issues associated with the usability of the healthcare devices. As is evident from the pattern of cyber-attacks, most of the cybersecurity vulnerabilities cases have happened in the present period. Just recently when the whole world was fighting with the COVID-19, then the hackers were hacking the UK based healthcare facility which was helping in the CORONA vaccine testing.

5 Healthcare Data Breaches

According to a report published by JSP, there was a phenomenal increase of 62% in the use of network connected healthcare devices, the highest in the last five years. This figure is expected to reach 25 million now. Since, the devices and databases connected with the Internet can be easily accessed for expediting the treatment, more and more patients are now availing their services. However, with more users of the technology, the risk of cyber threats is also increasing. Though 35% of the patients expressed trust in the use of the healthcare devices, 65% of the patients had concerns about their data being corrupted in case of software vulnerabilities or data tampering.

Health Insurance Portability and Accountability Act (HIPAA) is a public law 104–191, and second privacy rule promulgated by the USA in 1996. HIPAA conducted a study on healthcare data breaches, data lost in the breaches and settlement and penalty cost borne by the hospitals. In our study, we have organized data from 2009 to 2020. Year-wise comparison of attacks shown in the Fig. 2 graph highlights the compelling need for effective safeguards against attacks to maintain integrity, availability and confidentiality of healthcare data. HIPPA and NetSec have released an exhaustive report on the episodes of healthcare data breaches in the last ten years data [18]. We have categorized the types of attacks that

have usually happened in healthcare. In 2019, Zoll, a healthcare device vendor, notified that 277,319 patients' personal healthcare data was lost due to the error at the time of server migration.

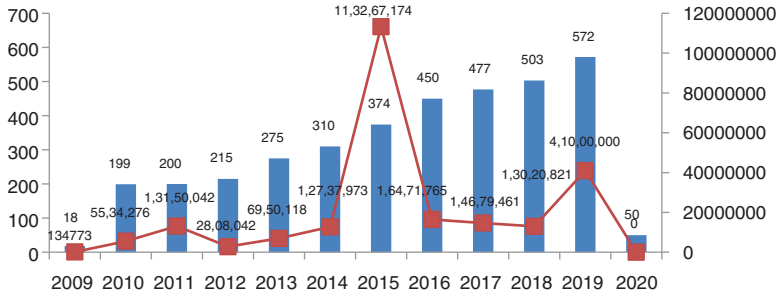

Figure 2: Number of breaches and data losses

Security regulations and laws have failed to protect the patients' data from being invaded and breached. Newly developed threats on the electronic health data require more revisions in HIPAA so as to provide effective counter measures and stringent penalties for the violators. In addition to the crisis of intentional data pilfering, there are also several other reasons for loss of data. These factors could be human error, flaws in the software, system failure, hardware failure and natural disasters. At present mail phishing is the biggest cause of data breaches in healthcare. Main challenges for healthcare device security are software threats. Through the MEDJACK, the malware attackers can access the networked devices and control the connected devices. For the safety of the device, the operating software must be consistent.

As per the report generated on 23 July, 2019, the maximum number of patients' records was compromised in 2015 (Protenus Breach Barometer). In 2009, the total number of breaches was 18 shown in Fig. 2, and compromised data was 134773 and in 2010, the data breaches suddenly increased by 11 times. From 2010 to 2011, there was an increment of just one instance but the records increased by 3 times. In 2012, there were 215 breach episodes but the count of the exposed records decreased. This was the lowest number of compromised data. In 2013, the total breaches were 275 and data lost was 6,950,118 and in 2014, the data breaches were 310, with 12,737,937 records exposed. In 2016, it was 450 and a total of 16,471,765 records were compromised. In 2017, the figure reached 477 and data compromised was 14,679,461. In 2018, 503 breaches occurred and compromised data numbers reduced to 13,020,821. Most of the data breaches were caused by hacking, third party vendors and phishing. Also, this data has been shown in Fig. 2 and has been outsourced from netsec.news [18].

The healthcare data breaches recently released by the Protenus in 2020 report shows that 2019 was the worst in the context of data breach episodes. A total of 572 data breaches were identified in 2019 and data compromised was 41 million. Total numbers of breaches and numbers of data compromised has been shown in Fig. 3. Recently in January 2020, Walgreens reported about the data breaches in personal mobile messaging apps. This was due to an internal error that occurred on the app and personal data became viewable to the others users.

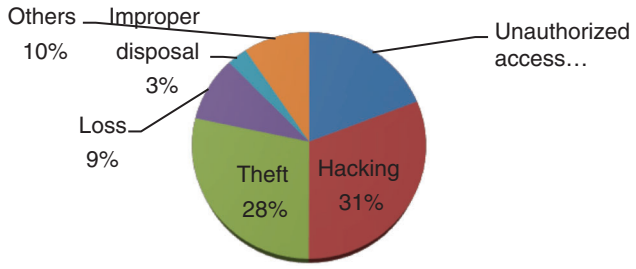

Figure 3: Healthcare data breaches

There are five main causes for the data breaches in the healthcare which are enumerated below:

5.1 Hacking

Remains the foremost cause for data breaches. Hacking usually happens through phishing emails sent by the attackers for infecting the system. Healthcare data breaches have continuously increased during 2018 to 2019 and hacking episodes have grown by 108%.

5.2 Data Theft

Data theft is the second main cause for the data breaches. Portable devices and other lighting come under theft. The theft event personal device or data become stolen respect to 2018 in 2019 42% decrements in theft of data

5.3 Data Breaches

Data breaches can also be initiated through *unauthorized access*. During 2018 to 2019, 41% of the data breaches happened because of the unauthorized access.

5.4 Loss and Improper Disposal

Loss and improper disposal of the old devices can also lead to data breach episodes [19,20]. Remaining 10% of data breaches occurred by other hacking events.

Fig. 3 shows the percentage of the cause of the breach which has been displayed through the pie graph. In this graph, 31% of the data breaches happened by hacking/phishing, rest of the 28% data breaches were caused by theft. The unauthorized access was 19%, and the last 10% of the breaches were initiated by other causes.

The failure of healthcare devices can have fatal consequences. Hence, whenever the defects have been detected, there has been a recall of the devices to analyse and rectify the errors. Recalls are divided into three classes. Class-I devices are more risky and dangerous for life; Class-II is partially risky for health and life; Class-III devices only violate the law of agency and are not threats to the patients [11] health. In 2009, a total of 48 devices were recalled. In 2010, the number of recalled devices increased to 60, in 2011, recalled devices were just 25. In 2012, this number reached 30; in 2013, there were 62 recalls, whereas in 2014, 59 recalls were recorded. In 2015, 2016, 2017, 2018, and in 2019, recalls done were 32, 40, 32, 32, and 48, respectively. All these recalls were only Class-I types of device recall.

The year-wise data of ransom, settlement and penalty cost in dollars and percentage of increment and decrement has been shown in Fig. 4 is the graphical representation of data settlement cost from 2009 to 2019. In the graph, we can see that the worst years were 2016, 2017 and 2018 with respect to settlement cost. In these three years, the total penalty cost was greater than the remaining year. In 2016, the cost was $23505300; and in 2017, the ransom demand reduced. Thereafter, in 2018, it rose to $28683400; the highest data settlement cost in five years [19].

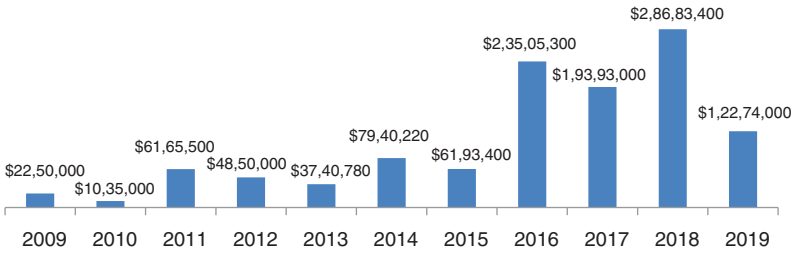

Figure 4: Settlement cost in dollars

In 2009, the settlement and ransom cost increased to 95% in comparison to 2008. And suddenly, in 2010, the settlement cost decreased by 117% in comparison to 2009. In 2011, the settlement cost increased by 82% in comparison to previous year. In all the years of settlement cost, the highest was in 2015 which was 280% more in comparison to 2014. Thereafter, in 2016, 2017, and 2020 there was 17% decrement, 47% increment and 52% decrement, respectively, in the settlement cost. Settlement cost is for data compromise and ransom and penalty on the healthcare centers and vendors by civil monetary penalty for HIPAA rules violations. Penalties imposed by HIPAA depend on the extent of violation. If the entity is unaware of the violation and makes an effort to correct, then the fine would be only $25000 per year [20]. If the entity is unaware about the violation and doesn't make any effort, then the penalty imposed would be $100,000 per year. In case of wilful neglect to be the cause of violation, and if corrected within 30 days, then the penalty imposed would be $250,000 per year. In case of wilful neglect to be the cause of fault and no efforts to rectify the error, the penalty imposed will be $1,500,000.

6 Future Predictions of Healthcare Data Breaches

Future prediction of data breaches up to 2024 has been done and depicted in Fig. 5. Future prediction has been done by polynomial equation order 6 for the breaches for next five years. We observed that the breaches are increasing till 2023 and in 2024, they will reduce and reach to 1240. In the forecasting of data breaches, we also observed that the next 3 to 4 years will be more difficult for the healthcare industry, because data breach episodes will increase to 1400 in the next 3–4 years. If the data breaches increase at this rate, then the healthcare industry will spend more money on the security of healthcare devices and data. For dealing with these security breaches in the forthcoming years, at least 20% more cybersecurity experts and well trained employees will be required globally. Because most healthcare centers do not their personal cyber experts, they hire third party cyber experts. Fig. 5 below shows the forecasting of data breaches.

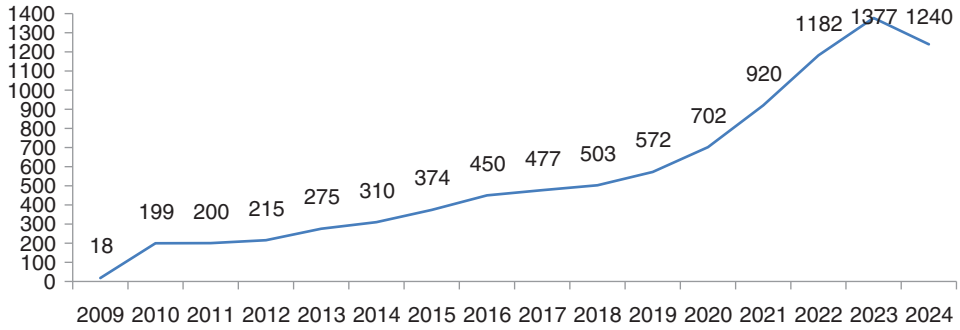

Figure 5: Future prediction of healthcare data breaches

Till 31 March 2020, 50 plus breaches have been done. If the breaches will increase at this rate, they can touch our breaches predictions which is 700 plus in 2020. Till 2023, the numbers are likely to reach the count of 1377. 2024 will be the relief year for the healthcare industry because the breaches will decrease to 1240. If there are as many as 1377 breach cases, then data and cost both will be affected. Authors have used here the polynomial order 6 model ($y = -0.0121x^6 + 0.5807x^5 - 10.689x^4 + 95.784x^3 - 430.38x^2 + 934.33x - 569.73$) for breaches forecasting. Authors opted for a polynomial order 6 model because this model is the most conversant one for the forecasting on the basis of previous year data breaches. We have input the previous data set in the polynomial model and predict the breaches for next 5 years based on previous breaches which are shown in the graph Fig. 5. Prediction of data breach cases in 2023 is approximately 1377. Forecasting of the data breaches will facilitate more research in this domain. A survey agency of cybersecurity observes that 84% of

the hospitals at present do not have their own security experts and they hire third party security experts. Such issues need immediate remedial interventions.

7 Discussion

Healthcare device security is a big challenge for the healthcare industry and vendors [21]. When the FDA allows devices in the markets, then they see it as an advantage for the patients. Disadvantages become apparent with the use of the devices. Though the threats and vulnerabilities that affect a healthcare device cannot be fully removed, minimising them is the need of the hour. If the healthcare industry adheres to FDA's guidelines and adapts the requisite safety norms, then the risks can be reduced to a great extent.

Authors have used here polynomial model ($y = -0.0121x^6 + 0.5807x^5 - 10.689x^4 + 95.784x^3 - 430.38x^2 + 934.33x - 569.73$) ($y = a + x^n$) for forecasting of healthcare device/data breaches till 2024. Polynomial model is more suitable then the other forecasting model like Trending model and exponential model. Here, the authors have shown the polynomial equation results only.

where;

a = the intercept, x = the explanatory variable,

n = the nature of the polynomial (e.g., squared, cubed, etc.)

Authors have used here the polynomial order 6 equation for data breaches forecasting. The Fig. 5 above shows the results of the forecasting of the data breaches. Polynomial graph in Fig. 5 follows the previous year's data and is rising continuously. However, the data breaches will reduce in 2024. Through the Fig. 5, we can see that the numbers of breaches are increasing year-wise in the above section. We have observed that no other research study has defined and explained the forecasting methods used in prediction of data breaches. In this article, the authors have justified and explained the methods that are used in the forecasting.

The contributions of the authors in this article, the authors have done the analysis of the studies which have been done in the past besides working on a separate analysis of the breaches, settlement cost, healthcare device maintenance cost based on CAGR (Compound annual growth rate) = 5.3% [22] annually by simple percentage calculation dl.acm.org/ a brief chronology (2020), forecasting of data breaches have been done by the polynomial model. The explorative approach undertaken for our research endeavour attempts to emphasise on the need for not only secure healthcare devices, but also maintenance issues that must be focused upon while manufacturing these devices technically and economically feasible.

8 Forthcoming and Open Security Challenges

There are several challenges and issues surrounding the functional safety, security, and essential performance of healthcare devices. These issues often arise due to the three main components of the healthcare devices: Hardware, software and network. Furthermore, the software issues of the healthcare devices include software security, network security, system and data security. In the healthcare device, malware and vulnerabilities are major issues. Issues arise with healthcare devices when a device communicates with the other device or network. Implantable healthcare devices have memory, processing power and battery power. All these features also create issues for security. Attackers mostly trying to prey on the vulnerabilities of networked devices and mainly focus on application software, database servers, and web servers.

Web Servers

Devices can configure and interact with other devices through the interface provided by the web servers. Mostly, web services often contain easily-susceptible vulnerabilities. Freely available hacking tools available on the internet are used by the hackers to expose the vulnerabilities and easily gain access to the device.

Database Servers

Mostly, healthcare organisations store patients' personal data for their use on databases. Data can be easily accessed only by the query or structured query language (SQL). This database is highly prone to attacks by the SQL injection. Through the SQL injection, the attackers simply alter and delete all information of the patients and staff from the database.

Application Software

Software contains many loopholes which make the software vulnerable. If the software has not been subjected to software vulnerability testing, then these flaws can be the source of data breach.

The three main challenges with healthcare device are:

8.1 Software Security Challenge

Software security is a critical feature in keeping the security of the healthcare device intact. FDA security communication enlists URGENT/11 cybersecurity vulnerabilities which may introduce risk in healthcare devices [4]. Software security challenges have the following crucial stages that need to be focused on:

8.1.1 Secure Development of Healthcare Device Software

Healthcare device Software development is the same as other software. For writing good and secure codes, it is imperative to train and impart knowledge to the security practitioners.

8.1.2 Update Mechanism and Patch

Healthcare device software contains code and third party software components. Third party software components may be the cause of vulnerabilities. Some of the healthcare devices (e.g., WannaCary, NotPetya, Orange-worm) are hacked through third party software. Patches are easily available and these patches update the software for making the device safe and secure. However, it is important to determine whether the source of the update is original or not. Confirming the authenticity of the source is an important task for safety of healthcare devices.

8.2 Hardware Security Challenges

Hardware security pertains to the designing and maintenance of healthcare devices. Hackers can install the vulnerable hardware and get access to the device. Following are the concerns that need attention:

8.2.1 Security of Data Storage Device

Data storage in healthcare devices is also unsafe; these devices require safety from internal attackers.

8.2.2 Security at Install and Replantable Parts of the Device

Most of the hardware device attacks occur at the time of maintenance, so precaution should be taken while replacing or installing any part of the device.

8.2.3 Internal Risk

Internal risk always arises on data and devices. Internal risks refer to involvement of the staff for data breaches.

8.3 Interoperability Security Challenge

Security issues can arise because of wireless communication over the network. Networked connected healthcare devices play an important role in healthcare. However, the data exchanged online can be exposed to the third party vendors who can safely hack or infect the data by malware and unauthorized access. When data is travelling over the network then trespassing also occurs on the data. So making the network secure for transmission of the data is also a major challenge and the aspects that need focus in this regard are:

8.3.1 Security of IPnet

IPnet is the network compatible software which is used in communication of devices. Most of the networked devices are hacked through IPnet [4].

8.3.2 Monitoring of Network Flood

Network flood also occurs in the networked devices. If a large amount of data travels over the network, there can be a problem in accessing the data. This problem usually arises because of DoS attacks.

9 Conclusion

Healthcare devices are an integral part of present day healthcare services. From the patients' imaging and diagnosis of the diseases to the treatment, healthcare devices are a key asset for the patients as well as the doctors. Since most of the healthcare devices nowadays are connected through the network, the vulnerabilities and cyber-attacks are also increasing. This paper overviews the medical device security, components and work done for security. And analyze and predict healthcare data breaches with the help of polynomial methods and find that hacking and theft events cover up to 50% of total data breaches. In our cost analysis we observe that the settlement cost is increasing year by year. This is a thinkable point why hackers targeting healthcare data. After that we have discussed the open security challenges of the medical device. Open challenges of this study will help the researchers in the research, maintenance cost prediction and data breaches settlement cost prediction also helps the manufacturing industries to focus on the technical and economical feasibility because this is the key point for the healthcare industries. The manufacturers of healthcare devices, healthcare professionals as well as cybersecurity experts must collate their efforts for inventing safer and secure digital healthcare aids for the patients.

Acknowledgement: This project was supported by Taif University Researchers Supporting Project No. (TURSP-2020/107), Taif University, Taif, Saudi Arabia.

Funding Statement: Funding for this study is received from Taif University Researchers Supporting Project No. (TURSP-2020/107), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Digital Health Software Precertification Program, "Food and Drug Administration," Spring, MD: U.S. Food & Drug Administration, 2018. [Online]. Available: https://www.fda.gov/HealthcareDevices/DigitalHealth/DigitalHealthPreCertProgram/default.htm.

[2] D. Papp, Z. Ma and L. Buttyan , "Embedded systems security: Threats, vulnerabilities, and attack taxonomy," in *13th Annual Conf. on Privacy, Security and Trust*, vol. 5, pp. 145–152, 2015.

[3] M. Schiefer, "Internet of Things: Security evaluation of nine fitness trackers," Magdeburg, Germany: AV TEST, The Independent IT Security Institute, 2015. [Online]. Available: https://www.av-test.org/fileadmin/pdf/publications/avtest_2015-06_fitness_tracker_english-1.pdf.

[4] FDA Safety Communication, "URGENT/11 cybersecurity vulnerabilities in a widely-used third-party software component may introduce risks during use of certain healthcare devices," 2020. [Online]. Available: https://www.fda.gov/healthcare-devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce.

[5] A. Thorogood, S. Touré, J. Seydina, A. Hall and B. Knoppers, "Genetic database software as healthcare devices," *Human Mutation*, vol. 39, no. 11, pp. 1702–1712, 2018.

[6] E. Venera, "New firewall to safeguard against healthcare device hacking," Purdue University News Service, 2012. [Online]. Available: https://www.purdue.edu/newsroom/research/2012/120412RaghunathanHacking.html.

[7] M. Alenezi, R. Kumar, A. Agrawal and R. A. Khan, "Usable-security attribute evaluation using fuzzy analytic hierarchy process," *ICIC Express Letters–An International Journal of Research and Surveys*, vol. 13, no. 6, pp. 453–460, 2019.

[8] R. Kumar, S. A. Khan, A. Agrawal and R. A. Khan, "Security assessment through fuzzy Delphi analytic hierarchy process," *ICIC Express Letters–An International Journal of Research and Surveys*, vol. 12, no. 10, pp. 1053–1060, 2018.

[9] A. Agrawal, M. Alenezi, S. A. Khan, R. Kumar and R. A. Khan, "Multi-level Fuzzy system for usable-security assessment," *Journal of King Saud University—Computer and Information Sciences*, Elsevier, pp. 1–9, 2019.

[10] K. Fu and J. Blum, "Controlling for cybersecurity risks of healthcare device software, biohealthcare instrumentation & technology: cybersecurity in healthcare," *Biomedical Instrumentation & Technology*, vol. 48, no. s1, pp. 38–41, 2014.

[11] MEDJACK.4, "MEDJACK.4: Healthcare device hijacking," TrapX Security, 2018. [Online]. Available: https://trapx.com/wp-content/uploads/2018/04/MedJack.4.pdf.

[12] R. Kumar, S. A. Khan and R. A. Khan, "Durability challenges in software engineering," *Crosstalk*, vol. 29, no. 5, pp. 29–31, 2016.

[13] R. Kumar, S. A. Khan, A. Agrawal and R. A. Khan, "Measuring the security attributes through fuzzy analytic hierarchy process: Durability perspective," *ICIC Express Letters-An International Journal of Research and Surveys*, vol. 12, no. 6, pp. 615–620, 2018.

[14] IT Security News, "Cybersecurity," 2020. [Online]. Available: https://www.fda.gov/healthcare-devices/digital-health/cybersucity.

[15] NETSEC , "Healthcare data breach report," NETSEC News, 2020. [Online]. Available: https://www.netsec.news/2020-healthcare-data-breach-report.

[16] Healthcare Security, "Main causes of security breaches in the healthcare industry," 2020. [Online]. Available: https://blog.rsisecurity.com/main-causes-of-security-breaches-in-the-healthcare-industry/.

[17] HIPPA, "Healthcare data breaches statistics," *HIPPA Reports*, 2020. [Online]. Available: https://www.hipaajournal.com%2Fhealthcare-data-breach-statistics%2F.

[18] A. Algarni, M. Ahmad, A. Attaallah, A. Agrawal, R. Kumar *et al.,* "A fuzzy multi-objective covering-based security quantification model for mitigating risk of web based medical image processing system," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 1, pp. 481–489, 2020.

[19] CISION PR NEWSWIRE, "Global healthcare devices market report 2017-2024 market is expected to rise with the CARG of about 5.3%," *Wire News*, 2020. [Online]. Available: https://www.prnewswire.com.

[20] A. Agrawal, M. Zarour, M. Alenezi, R. Kumar and R. A. Khan, "Security durability assessment through fuzzy analytic hierarchy process," *PeerJ Computer Science*, vol. 5, no. 5, e215, 2019.

[21] R. Kumar, M. Alenezi, M. T. J. Ansari, B. Gupta, A. Agrawal *et al.,* "Evaluating the impact of malware analysis techniques for securing web applications through a decision-making framework under fuzzy environment," *International Journal of Intelligent Engineering and Systems*, vol. 13, no. 6, pp. 94–109, 2020.

[22] K. Sahu and R. K. Srivastava, "Needs and importance of reliability prediction: An industrial perspective," *Information Sciences Letters*, vol. 9, no. 1, pp. 33–37, 2020.

[23] S. A. Khan, M. Alenezi, A. Agrawal, R. Kumar and R. A. Khan, "Evaluating performance of software durability through an integrated fuzzy-based symmetrical method of ANP and TOPSIS," *Symmetry*, vol. 12, no. 4, pp. 1–15, 2020.

[24] K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Hesitant fuzzy sets based symmetrical model of decision-making for estimating the durability of web application," *Symmetry*, vol. 12, no. 11, pp. 1770–1792, 2020.

[25] K. Sahu and R. K. Srivastava, "Revisiting software reliability," *Data Management, Analytics and Innovation*, vol. 802, pp. 221–235, 2019.

[26] A. Attaallah, M. Ahmad, A. H. Seh, A. Agrawal, R. Kumar *et al.,* "Estimating the Impact of COVID-19 Pandemic on the Research Community in the Kingdom of Saudi Arabia," *Computer Modeling in Engineering & Sciences*, vol. 126, no. 1, pp. 419–436, 2021.

[27] K. Sahu and R. K. Srivastava, "Soft computing approach for prediction of software reliability," *ICIC Express Letter*, vol. 12, no. 12, pp. 1213–1222, 2018.

[28] A. Baz and H. Alhakami, "Fuzzy based decision making approach for evaluating the severity of COVID-19 pandemic in cities of kingdom of saudi arabia," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1155–1174, 2021.

[29] A. Agrawal, A. H. Seh, A. Baz, H. Alhakami, W. Alhakami *et al.,* "Software security estimation using the hybrid Fuzzy ANP-TOPSIS approach: Design tactics perspective," *Symmetry*, vol. 12, no. 4, pp. 1–21, 2020.

[30] R. Kumar, A. K. Pandey, A. Baz, H. Alhakami, W. Alhakami *et al.,* "Fuzzy-based symmetrical multi-criteria decision- making procedure for evaluating the impact of harmful factors of healthcare information security," *Symmetry*, vol. 12, no. 664, pp. 1–23, 2020.