International Journal of Current Research and Review
DOI: http://dx.doi.org/10.31782/IJCRR.2020.121721

Scopus

Research Article

IJCRR
Section: Healthcare
Sci. Journal Impact Factor: 6.1 (2018)
ICV: 90.90 (2018)

IoMT: A Review of Open APS System Security for Type 1 Diabetes Mellitus

Jasvindir Singh[1], Nor Azlina Abd Rahman[2]

School of Computing, Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia.

ABSTRACT

Background: To improve the health of patients, the Internet of Medical Things designates the interconnection of communication-enabled medical grade devices and their incorporation into broader health network. However, the Internet of Medical Things still faces significant challenges because of the critical nature of health-related systems, particularly in terms of reliability, safety and security.

Purpose: This research paper will present a brief overview of type 1 diabetes mellitus, as well as its current treatment modalities.

Results: In this regard, solutions in the view of problems patients face with current generations of insulin pumps are being discussed. Open APS (Artificial Pancreas System) attempts to reduce the burden of patients with type 1 diabetes by making a relatively safe and effective basic artificial pancreas system widely available. Besides that, this research paper will also discuss potential vulnerabilities that are faced by this system, as well as methods to overcome these issues.

Key Words: IoMT, Type 1 diabetes mellitus, Open APS, vulnerability, Attacks, Countermeasures

INTRODUCTION

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines equipped with unique identifiers (UIDs), and the ability to transmit data over a network without needing human-to-human or human-to-computer interaction1. In the broadest context, the word IoT includes anything that is connected to the Internet, but it is also used to circumvent it [1]. By combining connected devices with automated systems, it is possible to gather, analyze, and act upon information to help someone with a particular task or learn from a process. Thanks to the integration of various technologies, real-time analytics, machine learning, commodity sensors, and embedded systems the concept of the Internet of things has grown.

An IoT ecosystem is made of web-enabled smart devices that utilize embedded systems. For example, processors, sensors and communication hardware which are used in the collection, transmission and action on data that has been obtained from their respective environments. Sensory data acquired is then shared through IoT devices to be analyzed through the cloud or locally through a connection with an IoT gateway or another edge device. Communication with other related devices can take place, with them being able to act based on information shared between another.

Web-enabled devices utilize multiple protocols for connectivity, networking and communication, which are dependent on the specific IoT applications that were deployed.

IoT data collection operations can be made more efficient through both artificial intelligence (AI) and machine learning. Figure 1 shows the IoT system infrastructure as a general.

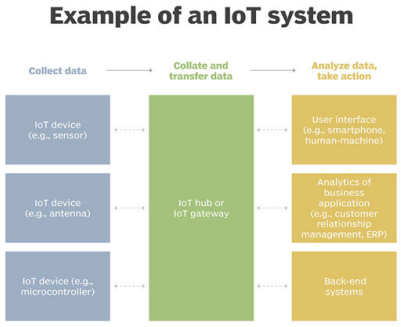

Figure 1: The Architecture of IoT System[1].

Corresponding Author:

Nor Azlina Abd Rahman, School of Computing, Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia; Email: nor_azlina@apu.edu.my

ISSN: 2231-2196 (Print) **ISSN:** 0975-5241 (Online)

Received: 22.06.2020 **Revised:** 23.07.2020 **Accepted:** 16.08.2020 **Published:** 08.09.2020

The internet of things assists people in both daily livings as well as work, allowing them to be in complete control. However, IoT doesn't just offer smart devices for home automation, it is also crucial for business. IoT gives businesses a real-time view of their systems and operations as well as providing an insight into everything, ranging from the efficiency of machines to supply chains and logistics operations.

IoT allows automation of processes and labour cost reduction for companies. The reduction of waste as well as improvements in service delivery lower production and shipment costs of goods with the added benefit of providing transparency into customer transactions. Therefore, the importance of IoT in everyday life cannot be understated and it will continue to grow as more businesses understand the benefits of having connected devices to keep them competitive.

Internet of Medical Things (IoMT)

The Internet of Medical Things (IoMT) is an IoT platform for medical and health-related uses, data collection and study analysis, and monitoring[2]. The term IoMT is referred to as "Smart Healthcare"[3], as the technology needed for establishing a digitized healthcare system as well as linking pre-existing medical resources and services.

IoMT devices facilitate both remote health monitoring and emergency notification systems such as simple devices that monitor heart rate and blood pressure to complex devices that monitor specialized implants, such as pacemakers or advanced hearing aids. Hospitals are even equipping "smart beds" that can track bed occupancy, abnormal patient movement as well as alter itself to apply the right amount pressure and support to the patient automatically without the interaction of hospital staff.

Specialized sensors can also be implemented in living spaces to monitor the health and general well-being of senior citizens, while also ensuring that adequate treatment is being provided as well as helping patients regain lost mobility through therapy[4].

A network of sensors created through these specialized sensors allows the collection, processing, transference, and analysis of important data in various environments, such as connecting in-home monitoring devices to hospital-based systems. Consumer devices that are used to promote a healthy lifestyle, such as connected scales or wearable heart monitors, are also possible through the IoMT. Antenatal and chronic patients can also rely on end-to-end health monitoring IoMT platforms to help in the management of health vitals and recurring medication necessities.

Advancements in the fabrication methods for plastic and fabric electronics have allowed the creation of extremely cheap, single-use IoMT sensors. The sensors, as well as the necessary RFID electronics for wirelessly powered disposable sensing devices, can be created on paper or e-textiles. Applications have even been designed specifically for point-of-care medical diagnostics where transportability and simplified systems are key.

As of 2018, IoMT is applicable in the clinical laboratory, healthcare as well as health insurance industries. IoMT in the healthcare industry serves its purpose in grouping attending medical staff as well as friends and family of patients in an organized structure, where data taken from patients is relayed to a central database, providing hospital staff easy access to all necessary patient information[5]. Moreover, IoT-based systems are patient-centric, which requires adapting to the patient's medical conditions. Within the insurance industry, IoMT serves to provide accurate and up to date types of dynamic information. This encompasses sensor-based solutions including biosensors, wearable, connected health devices, and mobile apps to monitor customer habits. This helps in improving underwriting accuracy and improved writing models.

IoMT can also be applied in healthcare to play an important part in handling chronic diseases as well as the deterrence and management of diseases. Through the use of connections between strong wireless solutions, remote monitoring helps medical practitioners log patient data as well as analyze them using intricate algorithms.

Type 1 Diabetes Mellitus and Current Treatments

Type 1 diabetes mellitus is a disease of insulin deficiency. It is a disease of childhood, reaching a peak incidence around the time of puberty, but can present at any age. Type 1 diabetes is generally considered to result from autoimmune destruction of insulin-producing cells (β cells) in the pancreas, leading to marked insulin deficiency. The incidence of type 1 diabetes is increasing: between 1960 and 1996, 3% more children were diagnosed worldwide each year. This is more common in countries closer to the Polar Regions, in general. For example, Finland has the highest Type 1 diagnosis rate per year at > 60 per 100 000 of the population, whereas in China, India and Venezuela the incidence is only 0.1 per 100 000. Type 1 diabetes is the most prevalent in Caucasians and the colder months, many patients are diagnosed. Diabetes is a major burden on health-care facilities in all countries. Globally, in 2015, diabetes caused 5 million deaths in those aged 20–79 years, and health-care expenditure attributed to diabetes was estimated to be at least 673 billion US dollars or 12% of total health-care expenditure[12]. The treatment of type 1 diabetes includes insulin therapy or pancreas transplantation.

Subcutaneous continuous insulin therapy

Subcutaneous continuous insulin therapy, commonly known as the insulin pump, is a system of insulin delivery that

uses a battery-operated medical device to deliver insulin continuously to the individual with type 1 diabetes. Device configurations vary between manufacturers but will include the pump with controls, processing module and batteries, a disposable insulin reservoir, and a disposable insulin set including a cannula for subcutaneous insertion and a tubing system to deliver insulin from the reservoir to the cannula. Some recent versions are disposable or semi-disposable and eliminate tubing from the infusion set (patch pumps). Insulin pumps allow the individual more flexibility with bolus insulin injections in both timing and shape, and also in changing basal insulin infusion rates. This is especially useful overnight when basal rates can be reduced to prevent low glucose but increased pre-dawn to prevent high glucose. Also, the temporary basal rates can be used to lessen the risk of hypoglycaemia with exercise. Determining an individual's basal rate on the pump requires help from a specialist, but in essence, is determined by fasting for periods of at least 4 hours while periodically evaluating the blood glucose levels and adjusting the pump infusion rate to maintain glucose in the normal range[12]. Basal rates will change and can be influenced by factors such as increased duration of disease, puberty, weight gain or loss, drugs that affect insulin sensitivity (e.g. glucocorticoids), and a change in fitness levels with exercise on overall glycaemia control. An example of an insulin pump is shown in Figure 2.

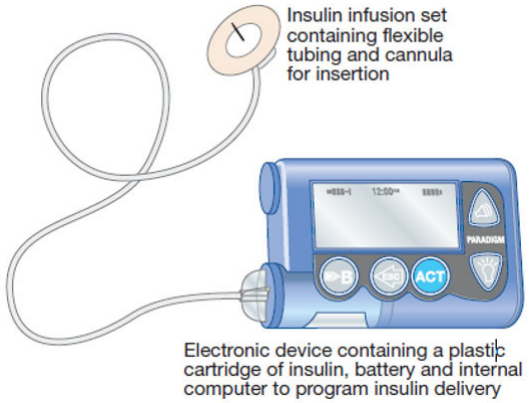

Figure 2: Insulin Pump [12].

Closed-loop insulin therapy

A further iteration in insulin pump therapy in recent years is the development of a 'closed-loop' system, also known as the artificial pancreas, as shown in figure 3. The artificial pancreas (AP) can vary in its set up and the different components employed in its delivery but core to an AP system are:

i. A continuous glucose monitor (CGM) measuring interstitial glucose levels every 5–15 minutes
ii. A smartphone (or personal glucose monitor) with an app that uses the glucose information from the CGM along with modifications inserted by the user to calculate how much insulin should be delivered. This is communicated wirelessly to the insulin pump
iii. The insulin pump that delivers insulin subcutaneously as directed.

These systems aim to integrate insulin pumps with continuous glucose monitoring systems (CGMS). In a closed-loop system, the CGMS device communicates with the insulin pump via a computerised program. This means that real-time glucose data obtained through the CGMS can be used to calculate an insulin dosage to be dispensed through the insulin pump (Figure 4). Features might include a 'low-glucose suspend' function, where detection of hypoglycaemia or a glucose level falling below a pre-set threshold (e.g. 4.0 mmol/L (72 mg/ dL)) signals the pump to stop dispensing insulin until the wearer can treat the hypoglycaemia with food or glucose tabs[12]. Current clinical trials in children and adults in the hospital or free-living setting aim to determine how effective this approach will be in optimising management of type 1 diabetes. Widespread use may, however, be limited by cost.

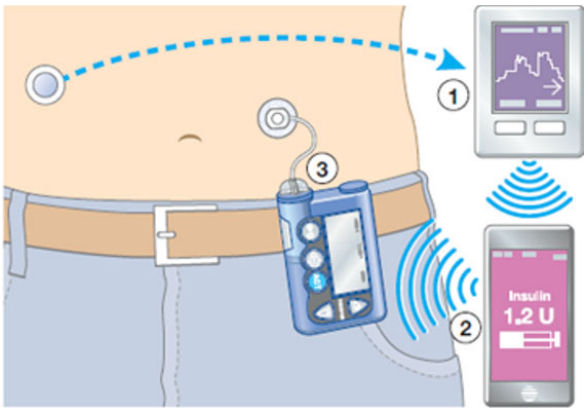

Figure 3: Artificial Pancreas [12].

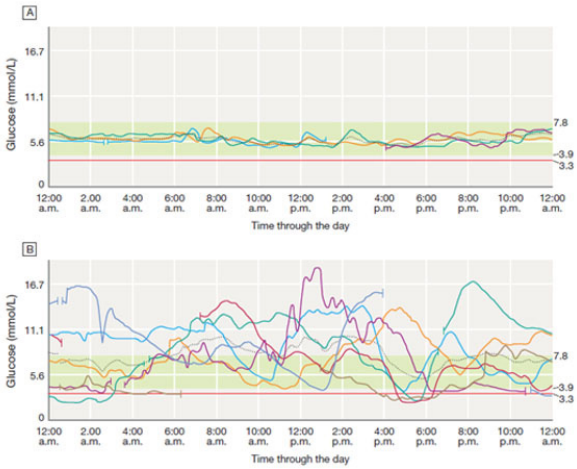

Figure 4: Continuous glucose monitoring (CGM) profiles: sensor data[12].

Graph A in figure 4 shows the CGM profile from an individual without diabetes while graph B shows the CGM profile from an individual with type 1 diabetes. The green box shows the reference range. CGM devices may be worn for 7–14 days and the glucose profile of each day illustrated by a different colour. Based on this, the person with diabetes and their health-care team can review overall profiles and adjust treatment as necessary to improve control and avoid hypoglycaemia.

Open Source Artificial Pancreas System (OpenAPS)

The Open Source Artificial Pancreas System (OpenAPS) is a relatively safe but potentially powerful, sophisticated however easily comprehensible, Artificial Pancreas System (APS) that is designed to automatically adjust an insulin pump's insulin delivery to always keep blood glucose in a safe range[11]. It does so by interacting with an insulin pump to obtain information of all previous doses of insulin (basal and boluses), by accessing a Continuous Glucose Monitor (CGM) to obtain current and accurate levels of blood glucose. It then issues instructions to the insulin pump to manipulate insulin dosing as needed.

OpenAPS differs from other APS that are currently in clinical trials in two major ways. Firstly, it is designed to use existing and approved medical devices, commodity hardware, and open-source software. Secondly, its design is focused on safety, understandability, and interoperability with existing treatment approaches and existing devices.

By taking this approach, OpenAPS has demonstrated to be both safer and more effective than current modern standalone insulin pump therapy, and more effective than the insulin-only hybrid closed loop and APS systems that have already been in clinical trials for years[11].

OpenAPS is designed to operate at any manufacturer with interoperable insulin pumps and CGMs. Older Medtronic or insulin pumps with either Dexcom or Medtronic CGMs are used in existing implementations. The same concept will also work with any manufacturer's insulin pumps that provide a way for the pump to issue temporary basal commands, and with any CGMs whose data can be retrieved in real time.

OpenAPS Vulnerabilities

The healthcare industry doesn't keep up with modern cybersecurity precautions[6]. Medical devices such as insulin pumps are highly vulnerable to cybercrime. Security is not the main concern in the development of a medical device, but rather its efficacy and potency in providing patient care. Thus, the majority of new medical devices are usually vulnerable. A list of possible vulnerabilities includes[7]:

i. Inadequate methods of authentication on the device. Attackers may gain unauthorized access onto the device as the device is unable to verify user identity. Attackers who were not supposed to gain access to the device in the first place can now access and modify settings in the device. As the device has a radio transmitter to connect to the network, it is vulnerable to unauthorized access and attack attempts. Examples of methods that attackers may use to gain access to the device include brute force attack, session hijacking, and sniffing.
ii. Lack of digital signing
The device has no way to cryptographically validate the legitimacy and integrity of software installed onto the device. Upon gaining access to the device, attackers may install malicious patches that let them alter the functionality of the device. This, in turn, may be used for harmful purposes.
iii. Lack of encryption on communications between the device and key fob.
Since it is relatively easy to determine the radio frequencies on which the key fob and pump communicate, attackers can easily reverse engineer the simple encoding and validity checks meant to protect the signal. Thus, enabling the attacker to capture the fob's commands. The attacker could then use readily available software to program a radio that is disguised as the fob and send commands that the pump will trust and execute.
iv. If the device already has a firewall, rootkits may allow concealment of malware from the user.
Rootkits can prevent a harmful process from being visible in the system's list of processes and keep its files from being read. Thus, the malware stays concealed and is not detected. The malware will then exploit security defects in the design of the operating system or application of the pump.
v. Once the attacker has bypassed normal authentication procedures, one or more backdoors may be installed to allow future access to the attacker.

One might only assume the intent of an attacker to hijack the device. If misused, they attacker may modify the device, causing insulin to be over- or underdelivered to the patient, leading to excessively low or high blood glucose levels, which eventually will lead to diabetic ketoacidosis, coma and finally death.

Possible Attacks

Multiple vulnerabilities have been discussed in the section above, and thus have highlighted a few key methods used in the process of hacking the device. Some of the methods used include:

i. Man-in-the-middle (MITM) attack:
A MITM attack is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. The attacker can intercept all

messages passing between the two parties and is able to inject new ones. A scenario involving this device might be when the user is trying to change settings in the pump. The user believes that whatever settings they applied to the pump will be in effect after having received confirmation from the device itself. However, they would probably not expect that an MITM attack is underway, and that the confirmation from the device is actually a telegraphed message from the attacker. Next, the attacker is free to manipulate the device, unnoticed by the user.

ii. Password attack:
A password attack is the process of recovering passwords from data that have been stored or transmitted by a computer system. There are multiple methods of such attack, including:

- Dictionary attack
Is an attack that takes advantage of the fact that people tend to use common words and short phrases as their passwords. The hacker uses a list of common words and tries them, often including numbers, against a list of usernames.
- Brute force attack
Is an attack that uses software to come up with likely passwords. These attacks start with common weak passwords and move on to more complex ones. The programs running these attacks would usually also attempt variations on upper- and lower-case characters.
- Traffic interception
Is an attack where the attacker uses software to monitor network traffic and capture passwords as they are keyed in.
- Key logger attack
Is an attack where the attacker manages to install software onto the user's device that tracks their keystrokes. This enables the attacker to gather usernames, passwords, as well as the place of logon.
- Social engineering attacks
Refers to a wide variety of methods to obtain personal information from users, such as phishing, spear phishing, baiting, and quid quo pro. All these methods are essentially used to dupe the user into providing the attacker with information otherwise believed by the user to be given to someone or something else.

iii. Malware attack:
Malicious software, more commonly known as malware, is a threat to devices and cybersecurity. It is software that attackers develop to gain access or cause damage to a particular computer or network, usually without the victim's knowledge. The software may be able to gain access to personal information or cause damage to the device. Types of malware include viruses, spyware, ransomware, and Trojan horses. Malware attacks can occur on a multitude of operating systems and devices. Malware attacks are consistently getting more sophisticated and becoming difficult to detect.

iv. Zero-day exploit:
Zero-day attacks are attacks on publicly known vulnerabilities that have not been patched. If discovered by attackers, an exploit will be kept secret for as long as possible and will probably circulate only through the ranks of hackers until software or security companies become aware of it.

Countermeasures

As multiple methods of attacking the device have been discussed, methods of defence for each will be discussed in this section

i. MITM attacks can be prevented and detected by two methods: authentication and tamper detection. Authentication will provide some degree of certainty that a given message has come from a legitimate source, while tamper detection would show evidence that a message may have been altered. A public key infrastructure (such as Transport Layer Security) may strengthen Transmission Control Protocol against MITM attacks. In such situations, clients and servers exchange certificates which are issued and verified by a trusted third party called a certificate authority. Use of mutual authentication, in which both the server and the client validate each other's communication, covers both ends of a MITM attack. However, the default behaviour of most connections is to only authenticate the server. Assessments are used to ward off MITM attacks as visual media is much more difficult and time-consuming to imitate than simple data packet communication. However, these methods will require a human in the loop to successfully initiate the transaction. Latency examination can potentially detect a MITM attack in certain situations[8]. To detect potential attacks, the pump and user access device can check for discrepancies in response times. If one of the two transactions between the two systems were to take an abnormal length of time to reach the other party, this could indicate that a third party could be interfering between the two, adding additional latency to the transaction.

ii. Strong passwords are usually the first defence against password attacks. According to the latest NIST guidelines[9], they recommend using passwords that are easy to remember and hard to guess. They recommend a good mix of upper- and lower-case characters, numbers, and special characters. Common words and phrases are to be avoided in a password. Site-specific words are not recommended. NIST also recommends checking passwords against a dictionary of known poor passwords. One of the best defences against social engineering tactics is educating the users on the various methods hackers use and how to recognize them. NIST also recommends not relying on passwords alone. Specifically, tools like single sign-on (SSO) and multi-factor authentication (MFA) should

be adopted in addition to passwords. The use of biometrics in place of a password makes false login nearly impossible.

iii. Training user on practices to avoid malware, as well as how to identify potential malware, can be beneficial in protecting a system. Security awareness training can keep users aware and observant. Controlling access to a system on the network would help ensure that the network is secure. Use of proven technology such as firewall, IPS, IDS and remote access through VPN would help minimize the routes of entry of an attack. Physical system isolation is also an option to consider, however in this case it is not recommended as the device would need networking functionality to be fully utilized. Regular scanning of the system in use for vulnerabilities and to detect if malware has been installed can help keep the device secure. Regular offline backups can also be created, in the case that recovery from a destructive virus has to be made.

iv. Zero-day vulnerabilities present a serious security risk, leading to potential damage to systems or personal data. The first line of defence against such attacks is to use comprehensive security software from reputable vendors. Next, users must be reactive towards installing new software updates when they become available from the vendor. These updates are usually pre-tested and have a higher chance of being useful than not. Updates should allow necessary revisions to the software or operating system and might include new features, remove outdated features, and most importantly fix security flaws.

Security Improvement of Current System

Since OpenAPS is only a reference design that is implemented into existing insulin pumps of other brands, they should firstly work with a sole manufacturer to produce their own devices. These manufacturers should design trustworthy devices and provide the documentation needed to demonstrate the trustworthiness of their devices in a premarket review by OpenAPS. To minimise the risk of multi-patient harm due to the lack of reliability, availability, credibility and confidentiality, these tools and systems should be configured to protect assets and functionalities. Protection mechanisms, in particular, will avoid any unauthorised use; ensure the integrity of code, data and execution; and, where necessary, protect data confidentiality. As part of premarket submissions, the manufacturer should submit documentation demonstrating how these design expectations are met.

i. Limit access to trusted users and devices only:
   - Limit access to the pump through the authentication of the user (preferably biometrics such as fingerprints)
   - Use automated timed methods to end sessions inside the programme for use in the environment where necessary (such as an immediate logout without input for 30 seconds by the user)
   - Employ a layered authorization model by differentiating privileges based on the user role (patient, physician, system administrator)
   - Use appropriate authentication (multi-factor authentication to permit privileged device access to system administrators and healthcare providers)
   - Strengthen password protection
   - Consider physical locks on pump and communication ports to minimize tampering when not in use.

ii. Authenticate and check authorization of safety-critical commands
   - Use authentication to prevent unauthorized access to pump functions and to prevent unauthorized software execution
   - Require user authentication before permitting software or firmware updates
   - Use cryptographically strong authentication on the device to authenticate users, commands, and all other communication pathways as applicable
   - Authenticate all external connections (to other devices for monitoring and updates)
   - Authenticate firmware and software. Verify authentication tags to authorized users
   - The device should be set to "deny by default" (e.g. to deny any unauthorized connections unless allowed)
   - The principle of least privilege should be applied to allow only the level of access necessary to perform a function

iii. Code Integrity
   - Only allow installation of cryptographically verified firmware or software updates.
   - Ensure that the new update is more recent than the currently installed version (to prevent downgrade/version rollback attacks)
   - Ensure that the integrity of the software is validated before execution based on digital signature

iv. Data Integrity
   - Verify the integrity of all incoming data (ensuring that it is not modified in transit or at rest)
   - Ensure capability of secure data transfer to and from the device and use methods for encryption and authentication of endpoints with which data is being transferred
   - Protect the integrity of data necessary to ensure the safety and essential performance of the device
   - Use current recommended standards (e.g. NIST) for cryptographic protection for communication channels

v. Design the device to detect cybersecurity events in a timely fashion
   - Implement design features allowing the detection, recognition, logging, timing and handling of security compromises during normal use the device should be designed to permit routine security and

antivirus scanning such that the safety and essential performance of the device is not impacted
- Ensure nature permits the collection of forensic evidence. The design should include mechanisms for generating and storing security event log files
- The device design should limit the potential impact of vulnerabilities by specifying a secure configuration (such as endpoint protection by anti-malware and firewalls)
- The device design should enable software configuration management and permit tracking and control of software changes to be electronically obtainable by authorized users
- The product life cycle should facilitate a variant analysis of vulnerability across different device models and product lines

vi. Design the device to respond to and contain the impact of a potential cybersecurity incident
- The device should be designed to notify users upon detection of a potential cybersecurity breach
- The device should be designed to anticipate the need for software patches and updates to address future cybersecurity vulnerabilities
- The device should be designed to facilitate the rapid verification, validation, and testing of patches and updates
- The design architecture should facilitate the rapid deployment of patches and updates

vii. Design the device to recover capabilities or services that were impaired due to a cybersecurity incident
- Implement device features that protect critical functionality and data even when it has been compromised
- The design should provide methods for retention and recovery of device configuration by an authenticated privileged user
- The design should specify the level of autonomous functionality any component of the system possesses when its communication capabilities with the rest of the system are disrupted
- The device should be designed to be resilient to possible cybersecurity incident scenarios

CONCLUSIONS

While healthcare technology plays a critical role in our population's health, they are prone to security threats due to interconnected, effortlessly accessible access points, outdated structures, and a lack of emphasis upon cybersecurity. Focus has tended to be positioned upon patient care; however, healthcare technology holds a large amount of valuable and sensitive data. If critical health systems are attacked, human lives are at risk. An attack could result in the loss of functioning of critical equipment. Concern has been further increased by "white hat" identification of health technology security weaknesses, which suggest that the remote manipulation of medical devices such as insulin pumps is a possibility. Cybersecurity is an essential part of maintaining the safety, privacy and trust of patients. More money and effort should be invested in ensuring the security of healthcare technologies and patient information. Security must be designed into the product from conception and not be an afterthought. Cybersecurity should emerge as an integral part of patient care culture.

Acknowledgements: The authors also wish to express gratitude to the management of Asia Pacific University of Technology & Innovation (APU) for their support.

Conflict of interest: The authors involved in the current study does not declare any competing conflict of interest.

Funding and Sponsorship: No fund or sponsorship in any form was obtained from any organization for carrying out this research work.

REFERENCES

1. Rouse, M. (2019). What is internet of things (IoT)? - Definition from WhatIs.com. [online] IoT Agenda. Available at: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT [Accessed 20 Feb. 2020].
2. da Costa, C.A., Pasluosta, C.F., Eskofier, B., da Silva, D.B. and da Rosa Righi, R. (2018). Internet of Health Things: Toward intelligent vital signs monitoring in hospital wards. Artificial Intelligence in Medicine, [online] 89, pp.61–69. Available at: https://www.sciencedirect.com/science/article/pii/S0933365717301367?via%3Dihub [Accessed 20 Feb. 2020].
3. Aboul, N., Hassanien, E., Bhatt, C., Suresh, A. and Satapathy, C. (2017). Studies in Big Data 30 Internet of Things and Big Data Analytics Toward Next-Generation Intelligence. [online] Available at: http://shsalmani.ir/wp-content/uploads/2017/09/Internet-of-Things-and-Big-Data-Analytics-Toward-Next-Generation-Intelligence.pdf [Accessed 20 Feb. 2020].
4. Istepanian, R.S.H., Hu, S., Philip, N.Y. and Sungoor, A. (2011). The potential of the Internet of m-health Things m-IoT for non-invasive glucose level sensing. [online] repository.lboro.ac.uk. Loughborough University. Available at: https://repository.lboro.ac.uk/articles/The_potential_of_Internet_of_m-health_Things_m-IoT_for_non-invasive_glucose_level_sensing/9548267 [Accessed 20 Feb. 2020].
5. Healthit.gov. (2018). What is HIE? | HealthIT.gov. [online] Available at: https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/what-hie [Accessed 20 Feb. 2020].
6. Kruse, C.S., Frederick, B., Jacobson, T. and Monticone, D.K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), pp.1–10.
7. Coventry, L. and Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, pp.48–52.
8. Aziz, B. and Hamilton, G. (2009). Detecting Man-in-the-Middle Attacks by Precise Timing. [online] IEEE Xplore. Available at: https://ieeexplore.ieee.org/document/5211025 [Accessed 20 Feb. 2020].

9. Nist.gov. (2019). NIST Special Publication 800-63B. [online] Available at: https://pages.nist.gov/800-63-3/sp800-63b.html [Accessed 20 Feb. 2020].
10. Health, C. for D. and R. (2019). Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. [online] U.S. Food and Drug Administration. Available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices [Accessed 20 Feb. 2020].
11. Anon, (n.d.). OpenAPS Reference Design – OpenAPS.org. [online] Available at: https://openaps.org/reference-design/ [Accessed 20 Feb. 2020].
12. Ralston, S.H., Penman, I.D., Strachan, M.W.J. and Hobson, R.P. (2018). Davidson's principles and practice of medicine. 23rd ed. Edinburgh: Churchill Livingstone/Elsevier.