Communications and Network, 2020, 12, 41-60
https://www.scirp.org/journal/cn
ISSN Online: 1947-3826
ISSN Print: 1949-2421

Risk Assessment Framework of mHealth System Vulnerabilities: A Multilayer Analysis of the Patient Hub

Mohammed Banu Ali[1], Trevor Wood-Harper[1], Abdullah Sultan Al-Qahtani[2], Abubakar Mohamed Ali Albakri[3]

[1]Institute of Innovation Research Innovation Management and Policy Division, University of Manchester, Manchester, UK
[2]UK Academic Consultations Ltd, Manchester Metropolitan University, Manchester, UK
[3]Birmingham City School of Computing and Digital Technology, Birmingham City University, Birmingham, UK
Email: mohammed.ali@manchester.ac.uk, atwh@manchester.ac.uk, Abdullah@ukaconsultations.com, Abubakar.albakri@mail.bcu.ac.uk

How to cite this paper: Ali, M.B., Wood-Harper, T., Al-Qahtani, A.S. and Albakri, A.M.A. (2020) Risk Assessment Framework of mHealth System Vulnerabilities: A Multilayer Analysis of the Patient Hub. *Communications and Network*, **12**, 41-60.
https://doi.org/10.4236/cn.2020.122003

Received: November 29, 2019
Accepted: March 7, 2020
Published: March 10, 2020

Abstract

Although there have been remarkable technological developments in healthcare, the privacy and security of mobile health systems (mHealth) still raise many concerns with considerable consequences for patients using these technologies. For instance, potential security and privacy threats in wireless devices, such as Wi-Fi and Bluetooth connected to a patient hub at the application, middleware and sensory layers, may result in the disclosure of private and sensitive data. This paper explores the security and privacy of the patient hub, including patient applications and their connections to sensors and cloud technology. Addressing the privacy and security concerns of the patient hub called for a comprehensive risk assessment by using the OCTAVE risk assessment framework. Findings reveal that the highest risk concerned data exposure at the sensory layer. In spite of the countermeasures presented in this paper, most served as a means to identify risk early as opposed to mitigating them. The findings can serve to inform users of the potential vulnerabilities in the patient hub before they arise.

Keywords

Confidentiality, Integrity, Vulnerability, mHealth, Internet of Things, Risk Assessment, OCTAVE

1. Introduction

The rapid increase in technology users, particularly personal computers and mobile devices has called for more robust network security systems [1]. This has raised many concerns regarding the potential vulnerabilities and threats that can disclose a user's or organisations sensitive data [2]. With respect to healthcare, restrictions on patient privacy in healthcare organisations (HCOs) become a greater risk [3] owing to the introduction of healthcare devices that are supposed to facilitate patient care and recovery. Given that potential network attacks have a greater impact on healthcare devices, such as sensors and patient applications, such technology can limit patients' ability to communicate their doctors and nurses. Therefore, mobile health systems (mHealth) play a key role in the ways of managing users' personal data, but at the same time, there are potential threats and vulnerabilities from Bluetooth and Wi-Fi technology that can manipulate mHealth systems to become a hindrance as opposed to a facilitator [4]. However, data security is a broad area comprising of many factors, such as authorisation, authentication, and surveillance with the intention of maintaining accountability, authenticity, availability, and integrity of online and mobile technologies [5].

Research Problem

Effective information security systems can protect a network by adhering to its intended purpose and take the necessary precautions to ensure the protection of private the sensitive data held by users and organisations. It is only then the needs of mHealth systems can be met through robust network security [6]. For example, traditional network protection like firewalls and encryption applications are insufficient to meet the security needs of organisations [7]. Consequently, there is a need to develop new architectures and tools to safeguard mobile computing applications and the wireless networks they rely upon [8].

For mHealth systems, there are three network layers that impact mHealth systems. These layers are the application layer, middleware layer and sensory layer [3]. While the application layer manages web applications hosted on the network, the middleware layer manages networking communication and the sensory layer manages wireless communication. One such wireless technology that utilises these three layers is known as the "patient hub". The patient hub is an integrated care platform that relies on wearable sensors [9] and smart cloud computing technology [10] [11] [12] [13] to support patients with Chronic Obstructive Pulmonary Disease (COPD) and co-morbidities, with specific emphasis on Chronic Heart Failure, Diabetes, Anxiety and Depression. However, the manipulation of the patient hub applications and disclosure of sensitive data through potential network attacks could be fatal for patients relying on these technologies.

Network security threats take many shapes, such as viruses, malware and spyware, in addition to other custom attacks from hackers. This raises a serious issue for mHealth systems that must be addressed for the sake of not only protecting patients' data, but also their lives. Given the great reliance of mHealth systems to support patient care, this calls for an assessment of security systems and networks. It is imperative to first identify the common threats to modern network infrastructures in mHealth system and to then determine how these threats can be mitigated. The patient hub as a contextual example is to assess the vulnerabilities in the hub's network. For that reason, this paper explores the vulnerabilities of modern networks that mHealth systems depend on, specifically the patient hub by conducting a thorough risk assessment to identify and mitigate potential security threats at the application, middleware and sensory layers.

2. Theoretical Background

2.1. IoT in Healthcare

In 1999, Kevin Ashton developed the term "Internet of Things" (IoT) to describe a unique group of interoperable objects that connect with each other using radio-frequency identification (RFID) technology [14]. Today, IoT enables the internet to connect to sensors which are connected with various wireless devices, with the majority relying on IP-based communications. For mHealth systems, IoT offers efficient medical treatment for patients, whilst providing early prevention and remote monitoring. Here, individuals or objects are equipped with sensors, actuators, and Radio-Frequency Identification (RFID) tags in order to facilitate the access by patients' caregivers. In particular, Kaul [15] stated that patients' RFID tags or medical devices can be identified, read, localised and controlled by IoT applications. This gives IoT technology the opportunity to tackle the potential challenges that face the healthcare system [16].

There are several layers in the IoT architecture, starting from the technology layer at the bottom to the application layer at the top. The responsibility of the bottom layers is data capturing, while the top layers manage application data and usage [17]. Since this paper focuses on the patient hub, emphasis is placed on the three main layers: application layer, middleware layer and sensory layer.

The application layer supports a number of IoT applications via two sub-layers [18]. The first sub layer is data management, which offers services ranging from Quality of Service (QoS) and cloud-computing technologies to data processing and machine-to-machine (M2M) services. The second sub-layer is application service, which is responsible for interfacing to end users and applications that run on the top IoT application layer. The middleware later is a software platform that provides networking communication services, ranging from access control and data filtering to device discovery and semantic data analysis. The sensory layer supports all wireless communication, including data encryption and signal detection [3]. Patient IoT applications rely on the sensory layer to gather and analyse large amounts of health data.

Wireless connectivity provides endless flexibility to mHealth devices connected to the organisational hub as a means to communicate with sensors, cloud services and other mobile gateways in addition to healthcare providers [19]. Google Health services, for example, is a mHealth device that can be used to interact with remote users. Mobile sensors connected to the organisational hub has the ability to communicate with a mobile gateway e.g. smartphones among other sensors [20], which can communicate remotely with other remote services for the purpose of storing healthcare data on a cloud platform, monitoring patients' vital signs and health conditions in the event of an emergency and archiving healthcare data in a database.

A benefit of transferring data to the organisational hub using mobile sensors is the minimal amount of manual data entry required to complete the data entry process, thus minimising cost, human error and ultimately increase system reliability. Despite the potentially reliable nature of wireless communication in mHealth devices, they can simultaneously create numerous challenges, such as high risk of system attacks and vulnerabilities associated with data security and privacy [21]. Some of the well-known privacy concerns for users of IoT applications stem from cyber-attacks, eavesdropping, data confidentiality, location privacy, disclosure of privacy and threats to data storage [3] [22]. The most significant types of security threats affecting mHealth systems are explained below.

2.2. Security Threats & Attacks

A number of studies have categorised network security threats where four different groups have been identified: structured threats, unstructured threats, internal threats and external threats [19] [23] [24] [25].

Structured threats refer to threats that are associated with highly experienced and proficient hackers. Attackers use sophisticated hacking tools to penetrate networks, such as masking and key logging techniques that are able to break though secure networks and exploit anything stored on that network. Unstructured threats are often performed by amateur or inexperienced hackers who will attempts to exploit the network [26]. Unstructured attackers will therefore resort to hacking tools such as shell scripts and password crackers. On reflection, structured threats will incur a high risk compared to unstructured owing to the attacker's experience and the nature of the tools used [27]. Despite the nature of both types of attacks, by no means should one be treated differently or under estimated as they both could potentially place harm on a network infrastructure.

External threats refer to threats performed by individuals who are unauthorised to access the organisational hub and will use the internet as a tool to attempt to break through the network. These types of threats can be performed either by experienced or inexperienced hackers. Internal threats can be performed by individuals who already have access to the organisational hub. Similar to external threats, the extent of the damage caused by an attacker depends on the attacker's level of expertise [28]. Despite the nature of the different network security threats, they all have a common ground when it comes to the different attacks facing a given network e.g. device communication attacks, reconnaissance attacks, resource depletion attacks, replay attacks and external device mis-bonding attacks. Owing to the comprehensive nature of these types of attacks that cannot be fully captured in this paper, as well as the explicit focus on the three main security layers, **Table 1** summarises these attacks in order to add some context to the nature of network security threats in the organisational hub.

Table 1. Types of attacks in mHealth systems & impacts on the network layers [19] [23] [24] [25].

Attack Type	Description	Layer Affected
Device Communication Attacks	Highly proficient attacks performed by experienced hackers who have the ability to create their own structured attacks, which target communication protocols in mHealth devices.	Application layer Middle-ware layer
Reconnaissance Attacks	Administrators can easily overlook these types of attacks owing to the specific form this particular attack takes when penetrating the network. Reconnaissance attacks make noises that are commonly heard, thus making them difficult to detect. Attacks are often performed by hackers for the purpose of acquiring information and then launching a denial of service attack to cover any trace of the attack.	Sensory layer
Resource Depletion (RD) Attacks	RD attacks dissipate resources of mHealth devices e.g. storage, battery and bandwidth. For example, an insulin pump depends on the wireless glucose sensor to give an accurate dose of insulin to a diabetes patient, and if these devices were attacked, it could be fatal for patients as attackers could regulate the administration of insulin.	Middle-ware layer
Replay Attacks	Attackers use replay attacks to manipulate sensor readings to force users to make wrong decisions. For example, hackers can exploit the communication of the sensor that shows a high glucose level was administered to patient according to supplementary knowledge regarding the victim, but later the attack could retransmit the information that pretends to be accurate information. High administration may show up on the system, but in reality, the patient may have never been administered their insulin.	Sensory layer
External Device Mis-Bonding (DMB) Attacks	DMB attacks target the mobile gateway running the device platform. The platform is connected to smartphones on a network channel via Bluetooth or Wi-Fi. As a result, any application that is able to access the platform via the communication channel could masquerade as an insider that can steal private information. This can be detrimental for patients who rely on health monitoring apps (e.g. heart monitoring and blood sugar levels) as they could be given inaccurate information regarding their current state of health, whilst having their personal information stolen.	Application layer Middleware layer

Naveed *et al.* [29] found that out of 68 smart device apps that are able to establish external device connections, not a single app had the capability to perform app-to-device authentication. This demonstrates the vulnerability of devices connected to the organisational hub that could affect both patients and the network infrastructure of the organisational hub through increased risk of attack and exposure.

Overall, the number of mHealth applications has increased significantly within the past decade and yet there is no fully developed security and privacy framework to ensure data integrity and individual privacy. A clear framework could provide reassurances that individual privacy is preserved, while providing the opportunity to modify existing security and privacy policies that ensure both individual and technical protections against some of the world's most deadly network attacks. For mHealth devices, technological developments have led to the capability of exerting more control over these devices and applications hosted on the organisational hub, as well as preserve the protection of patient information. Thus far, the literature has identified both manned and unmanned attacks that can affect mHealth systems and devices, as well as the impact of IoT on the organisational hub in terms of security threats and vulnerabilities at the application, middle-ware and sensory layers. Since there is no clear framework or risk assessment typology to identify potential attacks in the organisational hub, this paper attempts to develop a risk assessment framework to tackle this existing problem. But first, in order to develop this framework, there is a need to define the supporting methodology.

3. Methodology

A qualitative risk assessment methodology has been adopted in this paper. It demonstrates the principles to assess and evaluate information security risks [30] [31].

Qualitative Risk Analysis

The qualitative risk assessment scores the degree of potential impact of a given threat e.g. high, medium or low and is able to assess all potential impacts, irrespective of their tangible or intangible nature. Qualitative risk analysis is therefore a potentially suitable methodology for the nature of the research problem as it utilises several interconnected elements, such as threats, vulnerabilities and controls [7]. OCTAVE, for example, is a specific methodology that could potentially help to tackle the research problem.

OCTAVE is a qualitative risk assessment methodology which consists of three phases [32]. The first involves establishing requirements or defining existing threats; the second involves identifying the vulnerabilities in the network infrastructure; and the third involves the identification and prioritisation of risks, in addition to developing mitigating strategies to overcome or at least minimise threats and implementing them using the best possible methods [33]. However, certain activities or criteria have to be met at each stage before moving on to the next to ensure that all potential threats are identified and mitigated. Therefore, OCTAVE is more suited to this paper as it can potentially maximise the identification and mitigation of patient hub threats and the comprehensive nature of the methodology ensures that a thorough risk assessment is conducted.

The Expected Value Matrix (EVM) that OCTAVE relies on is used to determine the expected value of risk. Although the impact and probability values are subjective and are applied to the EVM to achieve an overall value, the methodology does provide a highly detailed and comprehensive risk assessment. The formula used to calculate loss is: Loss = Impact/Consequence × Probability.

OCTAVE is the chosen IS risk assessment methodology to assess common security and privacy issues within the patient hub at the application, middle-ware and sensory layers. Figure 1 illustrates the OCTAVE process.

Although OCTAVE is a comprehensive risk assessment methodology through its ability to maximise risk identification and mitigation, there is a lack of flexibility which can be demonstrated through its lack of customisation. This is because OCTAVE can be adapted to align with an organisation's requirement, but not all risk activities have to be mandatorily achieved, which can impact the risk analysis' position of where it can fit into the methodology.

Despite the shortfalls of OCTAVE, the methodology aligns well with the research problem owing to its methodical process and ability to identify, prioritise and mitigate risk or network vulnerabilities early. OCTAVE can even monitor IS risks, which could help to identify and mitigate future risks or threats that arise from new technological developments. Having identified OCTAVE as the more suited risk assessment methodology to tackle the existing privacy and security threats in the patient hub, an actual risk assessment could now be conducted, which accounts for the application, middle-ware and sensory threats within the patient hub.

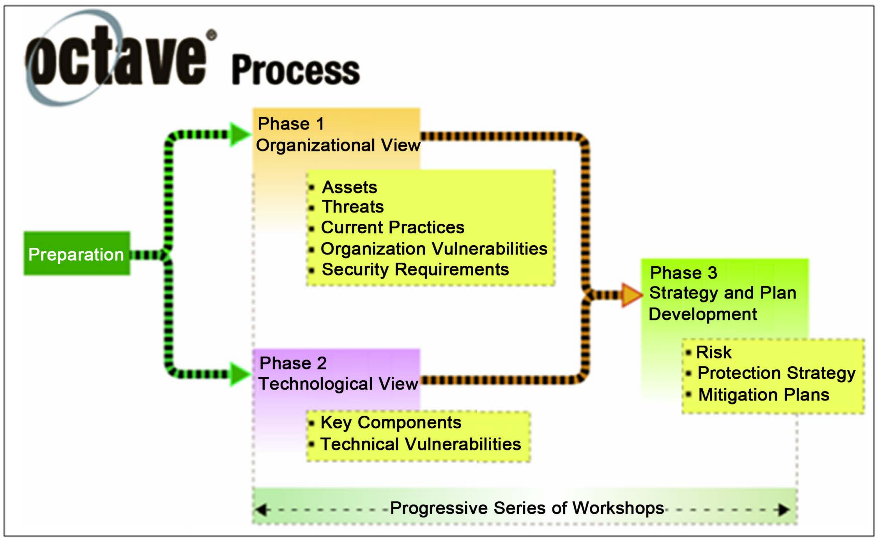

Figure 1. OCTAVE process [34].

4. Findings

As stated in the previous section, the OCTAVE method was adopted to support the risk assessment of the vulnerabilities and threats in the patient hub at the application, middle-ware and sensory layers. Figure 2 illustrates a typological process (inspired by OCTAVE) comprising of several steps that were followed to perform the risk assessment.

The steps followed (in order) are:

1) System Characteristics;
2) Threat Identification;
3) Vulnerability Identification;
4) Likelihood Determination;
5) Impact Analysis;
6) Risk Determination;
7) Control Recommendations.

4.1. Step 1: System Characterization

The patient hub is categorised in the following groups:

1) Hardware;
2) Software;
3) System Interfaces;
4) Data;
5) People.

The key components of the patient hub include WSNs, gateways, Internet, databases and users.

Figure 3 illustrates the patient hub architecture, which comprises of short-range wireless sensors, which can either be implanted or wearable devices.

Sensors in the patient hub are development around a light vest that comprises of standalone non-invasive chest sensors that help to monitor COPD and co-morbidities. A total of 26 sensors are used and are connected to a two-wire

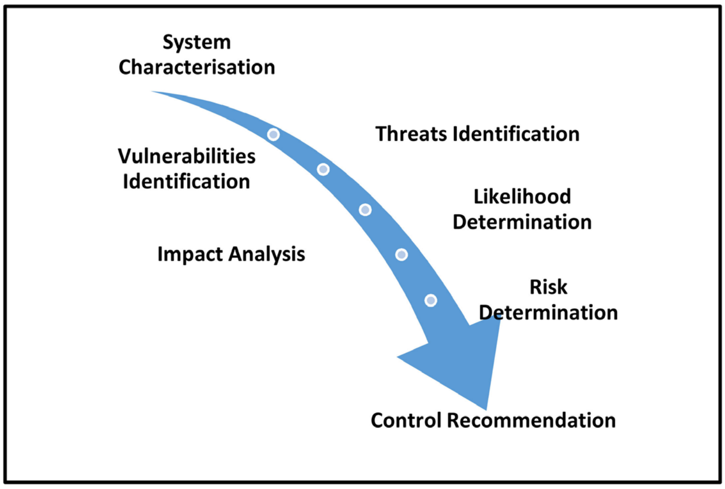

Figure 2. Risk assessment process.

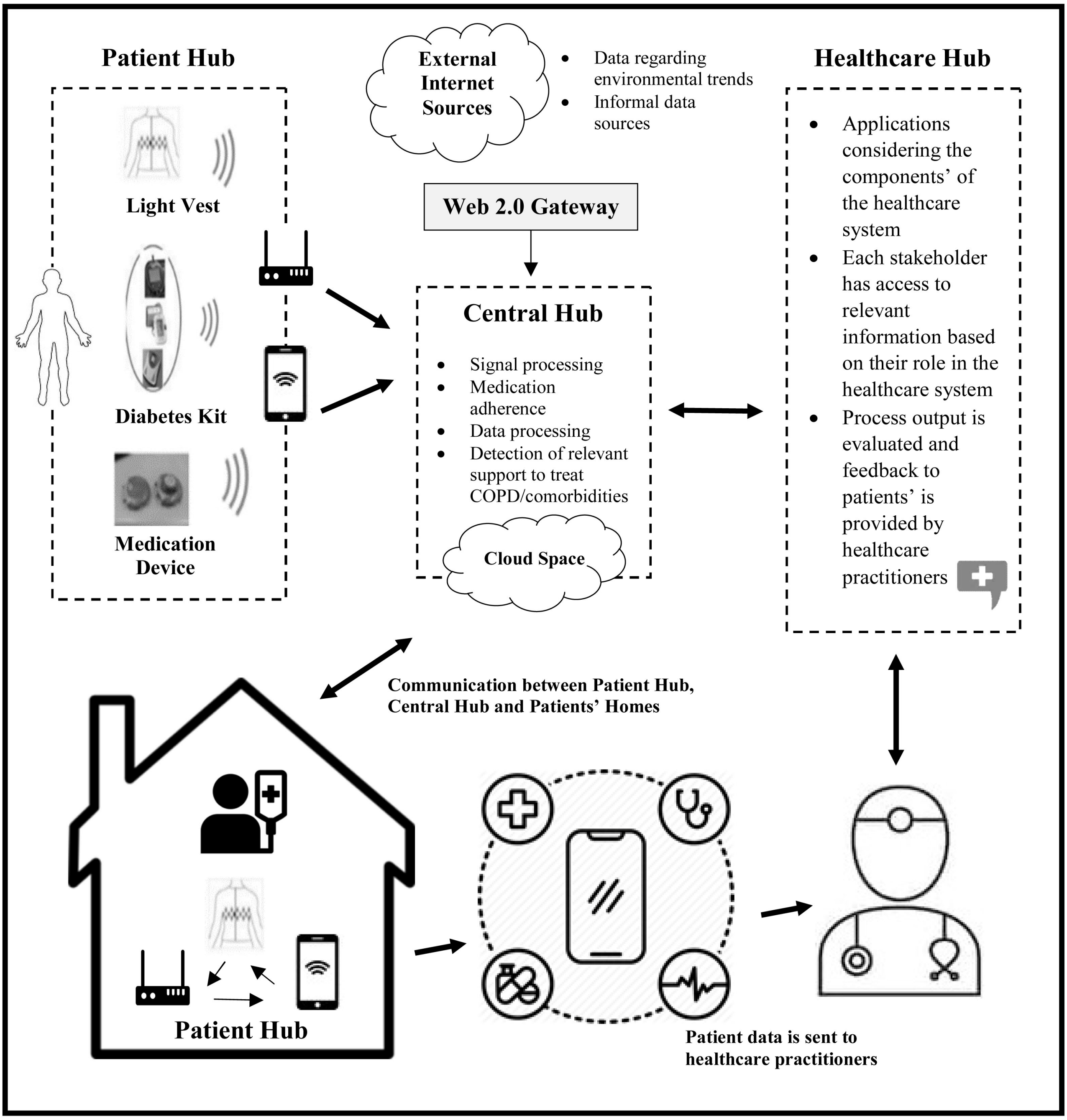
Patient Hub
Light Vest
Diabetes Kit
Medication Device
External Internet Sources
Data regarding environmental trends
Informal data sources
Web 2.0 Gateway
Central Hub
Signal processing
Medication adherence
Data processing
Detection of relevant support to treat COPD/comorbidities
Cloud Space
Healthcare Hub
Applications considering the components' of the healthcare system
Each stakeholder has access to relevant information based on their role in the healthcare system
Process output is evaluated and feedback to patients' is provided by healthcare practitioners
Communication between Patient Hub, Central Hub and Patients' Homes
Patient Hub
Patient data is sent to healthcare practitioners

Figure 3. Patient hub system architecture & application process.

Body Area Network (BAN). For diabetes patients, the patient hub includes a diabetes kit that has a weight scale, blood pressure meter and glucose meter.

In terms of the middleware platform, it runs the wireless sensor network (WSN) on the middleware layer, which is software-based. The WSN is enhanced through capabilities such as data processing, sensor data mapping and cloud data storage. The cloud database can operate internally or externally to the middleware layer and the data that is transmitted to the gateway is then transmitted to the middleware where it is stored in the database for future access. This also includes input devices that are able to access the documented data, such as mobile devices, personal computers and laptops among other devices that have the capability of connecting to a middle-ware platform.

On the software layer, users, such as nurses and doctors control software applications that allow access to the data stored on the database. The applications run on internet enabled devices (running on WLAN) such as computers, laptops and smartphones. Also, people who are connected to the patient hub project are often doctors and nurses, as well as patients and their families. Patient monitoring is carried out by the medical personnel. Patients who live at home are equipped with a WSN (via a gateway using the 802.15.4 protocol over a wireless medium) and their relatives, such as parents, children and legal guardians can have access to data under some legal constraints.

The WSN that collects the sensor data contains information regarding patients' health status (e.g. blood pressure) and their surroundings (e.g. room temperature). The database in the middleware layer stores the sensory data, and patients' records of past and present treatments and diseases, all of which can be accessed via an app.

In the patient hub, a number of assets have been identified ranging from hardware to software applications. However, the patient hub considers data the most important asset. However, replacing hardware equipment is costly. Compared to the loss of patient data, the inherent cost would be more important, particularly when it some down to legal compliance (such as healthcare regulation), the lack of patient privacy can have a negative impact on the organisation.

4.2. Step 2: Threat Identification

The next step involves the identification of threat-sources in the patient hub. A threat-source is essentially an event that has the potential to inflict harm on a system or network. Common threat-sources can be categorised as natural (e.g. floods and earthquakes), human (e.g. human error) and environmental (e.g. pollution and power-failure). Owing to the scope of this paper, which is patients' use of the patient hub and the threats they face, emphasis is placed on the human threat-sources. Human threats can be either unintentional or deliberate. Deliberate attacks are more malicious because they are often predetermined and aim to intentionally attack a network or system with the intention to control the network and disclose personal information. Human threats can come from either internal (e.g. medical personnel) or external (e.g. hackers and crackers) actors. In terms of the patient hub, both insider and outsider attacks can occur. Table 2 summarises both insider and outsider attacks that could compromise the patient hub.

Although money as a motivation may result in threat actions like data theft or eavesdropping, other motivational factors like unintentional errors can result in threats concerning intrusion, unauthorised system access and falsified data.

Figure 4 summarises the human threat-sources, their potential motivations

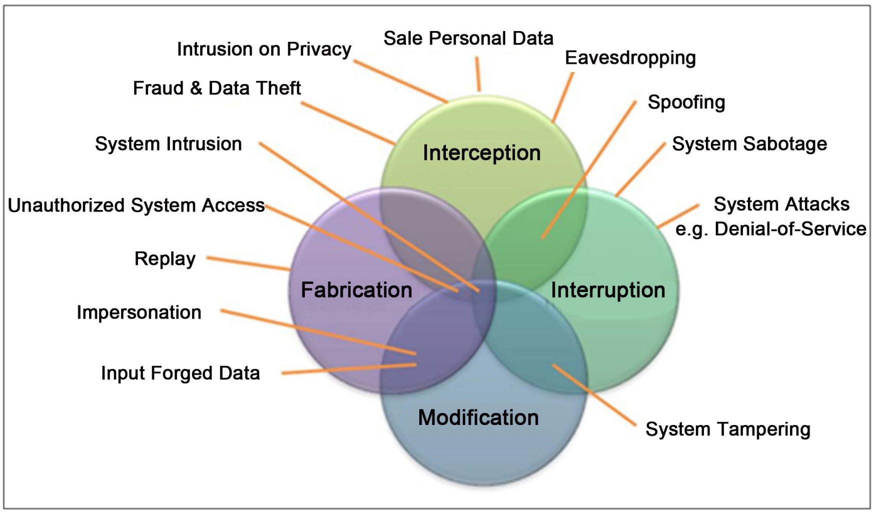

Figure 4. Threat classification.

Table 2. Threat statements, motivations & actions.

Threat-Source	Motivation	Threat Actions
Insiders Doctors, nurses, patients and families	Curiosity Intelligence Monetary gain Unintentional errors	Eavesdropping Fraud and data theft Input of falsified data Sale of personal data System intrusion System sabotage Unauthorised system access
Outsiders Hackers, companies and governments	Challenge/ego Destruction of information Illegal information disclosure Monetary gain Unauthorised data modification	Information theft Intrusion of privacy Replay, impersonation and interception Spoofing System attacks e.g. denial of service System intrusion System tampering Unauthorised system access

and threat actions. These threat-sources can be categorised as follows:

1) Interception: unauthorised parties gain access to protected assets;

2) Interruption: assets are lost, unavailable or unusable;

3) Modification: unauthorised parties gain access and tampers with assets;

4) Fabrication: unauthorised parties fabricate counterfeit objects to exploit the system and its assets.

4.3. Step 3: Vulnerability Identification

This step involves listing all the potential system vulnerabilities that come from the human centric threats identified in Step 2. Security experts need to be aware of the latest threats and vulnerabilities and thus it is important to identify them. However, it is not possible to provide a list of all potential vulnerabilities for software components, thus the rationale for focussing mainly on human threats.

Within the WSN are sensors that broadcast data via a wireless medium. Sensors have a smaller transmission range than traditional wireless devices owing to their weaker transmission power. Regardless of whether the threat-source is internal or external, they are equipped with an antenna to capture the data transmitted between sensors that are in clear transmission range. Therefore, antennas can create a vulnerability in the form of data theft.

Given that sensor nodes can be assessed physically in a hospital or a patients' home, they are more open to malicious entities that aim to steal (e.g. denial of service attack), insert (e.g. spoofing) or even destroy (e.g. sabotage) the sensors. As soon as an attacker has physical access to the sensor, they have the power to copy, modify and place software on new sensor nodes that can capture (e.g. data theft) or insert (e.g. sabotage) the forged data and make it look like a legitimate transaction. Sensors also have other constraints, such as limited battery power. Outside attackers prey on this vulnerability by exploiting the sensor to deplete a device's battery and this can be achieved through a denial of service attack. Therefore, the sensors become unresponsive as they rely on the device's battery power to function.

Viruses and Trojan horses are other attacks that enable attackers to access a database. If a database that is hosted on a server is physically accessible, the data can be easily exploited and compromised (e.g. copying private data). Vulnerabilities of this nature can be exploited for the modification, fabrication and theft of data and for infiltrating a network. Moreover, this is a gateway and middle-ware vulnerability since the data is transmitted from nodes to users without any protective measures. Therefore, these attacks exploit the confidentiality and integrity of sensory data (Table 3).

Table 3. Summary of system vulnerabilities & associated threat-sources & actions.

Vulnerability	Threat-Source	Threat-Action
Vulnerability 1: Sensor broadcast data on the wireless medium	Any internal or external entity	Data Theft, Intrusion on privacy
Vulnerability 2: Sensor nodes are physically accessible and not tamper resistant	Any internal or external entity	Destruction of sensors, Stealing sensors. Insert new sensors, Capture data, Spoofing, Generate false data
Vulnerability 3: Sensors are restricted devices	External entity	Denial of Service
Vulnerability 4: Data is stored in a database without means of encryption	Any internal or external entity	Data Theft, Intrusion on privacy, System intrusion, Destruction of data, Modification and Fabrication of data
Vulnerability 5: Data is transported through the System without encryption measures	Any internal or external entity	Data Theft, Destruction, Modification, Fabrication, Intrusion on privacy

4.4. Step 4: Likelihood Determination

This step involves the evaluation of the likelihood that an attacker exploits a vulnerability. Scores of high, medium and low are given to measure the likelihood of a vulnerability from a threat-source. The attacker's motivation, capacity and the effectiveness of existing controls helps to determine the likelihood level of a given threat-source. Table 4 summarises the three likelihood levels.

Furthermore, the European Directive 95/46/EC protects individual data (including healthcare data) by imposing protective rules for the autonomous processing, managing and distribution of data through sensors. Organisations are obligated to comply with the European Directive's regulations since the sensor data is a value asset. Using Table 4, a rating can be given to the vulnerabilities stated in step 4 and summarised in Table 4.

Antenna equipped with wave capturing technology is a hardware resource that enables attackers to eavesdrop on a system or network. Antennas are cheap or can be homemade with very little technical experience required to make them, making it one of the most efficient ways to exploit a network vulnerability. For example, the antenna attached to a device, such as a laptop enables the attacker to stand outside of a patient's home and secretly collect the information from the sensors. Given the cost effectiveness of implementing this vulnerability suggests the likelihood would be high.

Sensory attacks often require attackers to be physically close to the nodes and the nature of the threat-source determines how challenging the implementation of this vulnerability will be. Potential internal threat sources, such as social aid workers and relatives will often have a key to the patient's home or in a hospital scenario easy access to wards, adds to the trivialness of entering these settings. On the other hand, external attackers will have to illegally enter the premises and the difficulty of this depends on the setting, e.g. easier to sneak or break into a hospital as there are no alarms compared to a patients' home that could be rigged with a burglar alarm. In addition to entering the premises, the attacker must have strong technical knowledge about tampering with sensor nodes. Therefore, the likelihood of this vulnerability is medium as it depends on the attacker's technical proficiency and physical proximity.

A threat-source with a strong understanding of wireless devices and equipment is needed to exploit a sensory based vulnerability. Sensors that process signals from only trusted sources are potential controls that could be used to mitigate this vulnerability. Therefore, the likelihood of this vulnerability is low on the basis that the attack requires specialist knowledge and skills.

Table 4. Likelihood threat levels.

Likelihood Level	Description
High	Threat-source is highly motivated and sufficiently capable
Medium	Threat-source is motivated and capable
Low	Threat-source lack motivation or capability

The most vital and sensitive part of a system is data and is the reason why most attackers will focus on data that is held in databases. Methods that grant access to the database could be exploited to manipulate and destroy data, such as installing Trojan horses and viruses and even human error e.g. sharing passwords and installing malicious programs. Therefore, the likelihood of risk will be high as data is a valuable asset that can be used to expose people, obtain financial data and even patients' medical records, which attackers will prey upon.

Each component of a system can be used to perform attacks and compromise data through data theft and corruption. Existing communication channels offer very limited mechanisms to preserve data confidentiality and integrity, thus giving attackers the opportunity to eavesdrop between two internal systems components e.g. the gateway and middle-ware layer. Therefore, the likelihood of this vulnerability is high since an attacker can anywhere in the system and has multiple methods of performing attacks.

4.5. Step 5: Impact Analysis

The fifth step involves the determination of the adverse impacts resulting from vulnerabilities that have been successfully exploited. Similar to the likelihood scale, impact is also measured as high, medium or low. This helps to determine the risk levels for all identified vulnerabilities in step 4 through comparing the likelihood ratings against the impact analysis. Since the emphasis of this paper is on the data transmitted through the Patient Hub, only data-related vulnerabilities are measured. Table 5 summarises the impact categories.

A loss of confidentiality in patients' private data can arise from exploiting this vulnerability. Disclosing private medical data can lead to a loss of public confidence or individuals filing lawsuits against organisation as the regulations that are supposed to protect their data have been breached. With no security measures that can preserve data confidentiality and integrity, it can be difficult to gain users' acceptance of technology, thus resulting in a high impact of vulnerability.

Sensor nodes that are either stolen, destroyed or inserted can cause a number of problems, such as the integration of fake or false data and inaccessible sensory data. A loss of integrity and confidentiality can arise from the successful exploitation of this vulnerability e.g. destruction of sensory nodes prevents data transfer or rogue sensors transmitting data to the attacker. Monetary and cost impacts can also arise from stolen or destroyed nodes as they would need to be replaced. Therefore, the impact level of this vulnerability is high owing to the disruption it could bring to an organisation or individual.

Table 5. Impact levels description.

Impact Level	Description
High	Vulnerability could lead to loss of major assets or patient death or injury
Medium	Vulnerability could lead to a moderate loss of assets and medium risk or injury or death
Low	Vulnerability could lead to a minimal loss of assets and very little chance of injury or death

Unavailability of data and the transmission of corrupt data can arise from the battery exhaustion of a sensor. As soon as the sensor is running low on power due to a low battery, data accuracy is impeded. LEDs showing the battery level and sounds to indicate low battery power on a device are considered controls to prompt users to charge their device. Therefore, the impact of this vulnerability will be medium since low battery power leading to data interruptions can be quickly detected and mitigated.

Attackers who gain access to a database are able to steal, modify, insert and destroy the data stored within it. This vulnerability would again lead to further data integrity, confidentiality and integrity issues. This is because, for example, when an attacker eavesdrops on a wireless channel at a hospital, they will have full access to all patient data, which only they can manipulate. For that reason, the impact of this vulnerability will be high owing to the attacker's full access to patient data which they could disclose or sell.

A loss of data confidentiality and integrity can also arise from data having no protective measures, such as a VPN or firewall. Eavesdropping and the tampering of system components (e.g. middle-ware, gateway and sensors) is made easy without a firewall as attackers would be able to access a system that a decent firewall would have been capable of preventing. Therefore, the level of impact of this vulnerability will be high owing to a loss of the most valuable asset to a firm or individual, which is their data.

4.6. Step 6: Risk Determination

In step 6, an assessment of the level of risk to the analysed system is performed. This is measured based on the idea that a risk is function of the likelihood of a threat-source successfully exploiting a vulnerability and the degree of impact in the event of that exploit occurring. Risk levels are calculated by taking the likelihood and impact ratings and multiplying them together. Table 6 summarises how the risk levels are calculated based on both the likelihood and impact ratings (low, medium and high). The risk level leads to a subjective interpretation of the risk outcome, which is part of the qualitative risk assessment procedure owing to its highly descriptive nature.

Table 6. Risk level matrix: High (6 - 10), Medium (1 - 5) & Low (0.1 to 1).

Threat Likelihood	Impact		
	Low (1)	**Medium (5)**	**High (10)**
High	Low 1.0 × 1 = 1	Medium 1.0 × 5 = 5	High 1.0 × 10 = 10
Medium	Low 0.5 × 1 = 0.5	Medium 0.5 × 5 = 2.5	Medium 0.5 × 10 = 5
Low	Low 0.1 × 1 = 0.1	Low 0.1 × 5 = 0.5	Low 0.1 × 10 = 1

OCTAVE can help to avoid any confusion regarding the probabilities for the likelihood and impact levels. For the likelihood levels, each are given a level of 1.0 for high, 0.5 for medium and 0.1 for low. For the impact levels, each are given a level of 10 for high, 5 for medium and 1 for low. Table 6 outlines the resulting matrix, 0.1 - 1 being low, 1 - 5 being medium and 6 - 10 being high.

Table 7 summarises each risk level.

The risk level matrix helped to identify and determine the risk levels for each vulnerability. The resulting matrix illustrated in Table 6 shows that the level of risk in vulnerability 3 is low, a medium risk for vulnerability 2 and vulnerabilities 1, 4 and 5 represent the highest risk. For that reason, the seventh and final step recommends risk controls and mitigations.

4.7. Step 7: Control Recommendations

The previous steps identified a number of potential risks to the patient hub. This calls for countermeasures to mitigate these risks that aim to prevent or at least minimise the likelihood of risk occurrence, impact or both. Figure 5 illustrates the risk description based on the likelihood and impact of risk occurrence.

Vulnerability 3 which represents power restrictions in sensory devices is considered a low risk. Although users can overcome this risk through the trivial task of monitoring the device's battery power, providing additional countermeasures can be problematic owing the restrictions on sensors being inherent to the actual nodes.

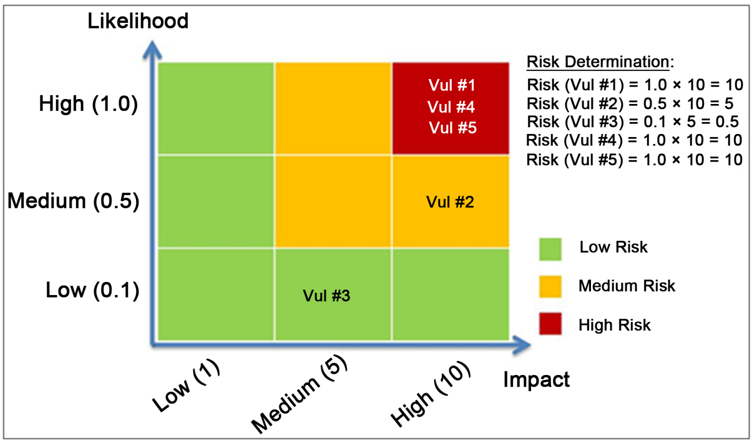

Figure 5. Risk description based on likelihood x impact of risk.

Table 7. Risk description.

Risk Level	Risk Description & Necessary Action
High	If an observation is assessed as high risk, correct measures are significantly required and corrective planning must be made as soon as possible
Medium	If an observation is assessed as medium risk, correct measures are moderately required and corrective planning must be made in a reasonable time frame
Low	If an observation is assessed as low risk, a decision has to be make whether corrective measures are required

Vulnerability 2 which represents the physical accessibility and tampering of sensor nodes is considered a medium risk. Similar to the low risks, there are very limited technical controls that can be used to mitigate this risk as it is based on the attackers' varying knowledge and skills of exploiting networks and systems, thus making it difficult to create a universal countermeasure. Alternatively, training patients about indoor security and installing a burglar alarm could help to reduce this risk.

Vulnerabilities 1, 4 and 5 represent a high risk. Sensory data could be protected against loss of integrity and confidentiality between the system components such as sensors, gateways and middle-ware layers, through data encryption in the WSN. However, these controls can only partly reduce the risks associated with the vulnerabilities 4 and 5 because these security measures cannot prevent data theft or modification if the system components are compromised. In other words, irrespective of all communication channels being secure, if a single component is malicious, the data remains insecure.

Mitigating the risk of vulnerabilities 1, 4 and 5 requires a security scheme that relies on cryptography, which provides endless data confidentiality from sensor nodes to data users. Also, given that the security challenge of the patient hub is huge, particularly in the application, middle-ware and sensory layers of the data cloud. The countermeasure here centers on the location of the patients sensitive data. For organisations that use the system, they will have its own unique hub and therefore will have a separate local database for storing sensitive data. Regarding the security of these databases, authorisation and authentication is needed by encrypting the access token of the system, which is stored in the local storage. In addition, HTTPS and VPN can be used to communicate between user applications, the patient hub and the cloud for additional protection. An SSL10 certificate can be used by the server to secure the data via encryption, thus enabling communication through an encrypted and secure channel.

4.8. Summary of Findings

According to these findings, the security of sensory data is lacking and no such framework exists to countermeasure this problem. Since existing security measures are failing to mitigate the risks, the preservation of security through the secure integration of wireless sensory networks in healthcare applications is a more suitable solution. This ensures that sensory data is protected against the unwarranted disclosure of data and loss of confidentiality among users.

Previously, a risk analysis of the patient hub was performed using the OCTAVE methodology. Despite the thorough risk assessment that was conducted, it was conducted via qualitative reasoning, meaning that the risk outcomes were based on subjectivity and predictions. In order to obtain a more objective risk assessment (based on likelihood and impact of risk), future studies could place more emphasis on statistical data. Though, theoretical findings suggest that statistics regarding the vulnerabilities in wireless sensory networks are scarce. Although previous studies have recommended countermeasures for

WSNs, they very rarely consider the likelihood and impact of sensory attacks. Overall, there is a need to preserve confidentiality and integrity of sensory data through the introduction of a cryptographic security scheme.

5. Conclusions

This paper aimed to identify and mitigate potential security risks in mHealth systems, namely the patient hub. Through an analysis of security impacts of mHealth systems, it was found that the security vision of the patient hub of using ubiquitous remote patient monitoring raises a number of security problems.

To address the research problem, the inherent risks of the patient hub were identified via the OCTAVE risk assessment methodology. Data exposure was found to constitute the highest risk. Integrating WSNs in the patient hub was found to provide a good solution to preserve data integrity and confidentiality.

Future research implications include studying the inherent risks of the patient hub using alternative risk assessment methodologies. These include: the Security Risk Management Discipline (SRMD), COSEO Risk Management Framework, ISO31000 series and the NIST Risk Management Framework. These frameworks could be used to replicate a similar process to the one presented in our findings to reveal any similarities and differences in their results.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Tewari, A. and Gupta, B. (2018) Security, Privacy and Trust of Different Layers in Internet-of-Things (IoTs) Framework. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2018.04.027

[2] Roozbahani, F.S. and Azad, R. (2015) Security Solutions against Computer Networks Threats. *International Journal of Advanced Networking and Applications*, **7**, 2576.

[3] Philip, N., *et al*. (2014) Design of a RESTful Middleware to Enable a Web of Medical Things. *EAI 4th International Conference on Wireless Mobile Communication and Healthcare*, Athens, 2014, 361-364. https://doi.org/10.4108/icst.mobihealth.2014.257408

[4] Vaidya, R.V. and Trivedi, D.K. (2017) M-Health: A Complete Healthcare Solution. *International Conference on Computing Methodologies and Communication*, Erode, 18-19 July 2017, 556-561. https://doi.org/10.1109/ICCMC.2017.8282527

[5] Radoglou Grammatikis, P.I., Sarigiannidis, P.G. and Moscholios, I.D. (2019) Securing the Internet of Things: Challenges, Threats and Solutions. *Internet of Things*, **5**, 41-70. https://doi.org/10.1016/j.iot.2018.11.003

[6] Faheem, K. and Rafique, K. (2015) Securing 4G/5G Wireless Networks. *Computer Fraud & Security*, **2015**, 8-12. https://doi.org/10.1016/S1361-3723(15)30036-1

[7] Whitman, M.E. and Mattord, H.J. (2014) Principles of Information Security. Cengage Learning, Boston.

[8] Janeček, V. (2018) Ownership of Personal Data in the Internet of Things. *Computer Law & Security Review*, **34**, 1039-1052. https://doi.org/10.1016/j.clsr.2018.04.007

[9] Munos, B., *et al.* (2016) Mobile Health: The Power of Wearables, Sensors, and Apps to Transform Clinical Trials. *Annals of the New York Academy of Sciences*, **1375**, 3-18. https://doi.org/10.1111/nyas.13117

[10] Ali, M. (2019) Cloud Computing at a Cross Road: Quality and Risks in Higher Education. *Advances in Internet of Things*, **9**, 33-49. https://doi.org/10.4236/ait.2019.93003

[11] Ali, M. (2019) The Barriers and Enablers of the Educational Cloud: A Doctoral Student Perspective. *Open Journal of Business and Management*, **7**, 24. https://doi.org/10.4236/ojbm.2019.71001

[12] Ali, M.B. (2019) Multiple Perspective of Cloud Computing Adoption Determinants in Higher Education a Systematic Review. *International Journal of Cloud Applications and Computing*, **9**, 89-109. https://doi.org/10.4018/IJCAC.2019070106

[13] Mohammed Banu, A., Trevor, W.-H. and Mostafa, M. (2018) Benefits and Challenges of Cloud Computing Adoption and Usage in Higher Education: A Systematic Literature Review. *International Journal of Enterprise Information Systems*, **14**, 64-77. https://doi.org/10.4018/IJEIS.2018100105

[14] Gawali, S.K. and Deshmukh, M.K. (2019) Energy Autonomy in IoT Technologies. *Energy Procedia*, **156**, 222-226. https://doi.org/10.1016/j.egypro.2018.11.132

[15] Kaul, S.D. and Awasthi, A.K. (2013) RFID Authentication Protocol for Medication Safety of Patients. *Journal of Medical Systems*, **37**, 9964. https://doi.org/10.1007/s10916-013-9979-7

[16] Medaglia, C.M. and Serbanati, A. (2010) An Overview of Privacy and Security Issues in the Internet of Things. In: *The Internet of Things*, Springer, Berlin, 389-395. https://doi.org/10.1007/978-1-4419-1674-7_38

[17] Atzori, L., Iera, A. and Morabito, G. (2010) The Internet of Things: A Survey. *Computer Networks*, **54**, 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[18] Jia, X., *et al.* (2012) RFID Technology and Its Applications in Internet of Things (IoT). 2*nd International Conference on Consumer Electronics*, *Communications and Networks*, Yichang, 21-23 April 2012, 1282-1285. https://doi.org/10.1109/CECNet.2012.6201508

[19] Zubaydi, F., *et al.* (2015) Security of Mobile Health (mHealth) Systems. 15*th International Conference on Bioinformatics and Bioengineering*, Belgrade, 2-4 November 2015, 1-5. https://doi.org/10.1109/BIBE.2015.7367689

[20] Triantafyllidis, A.K., *et al.* (2016) Framework of Sensor-Based Monitoring for Pervasive Patient Care. *Healthcare Technology Letters*, **3**, 153-158. https://doi.org/10.1049/htl.2016.0017

[21] Kearns, G.S. (2016) Countering Mobile Device Threats: A Mobile Device Security Model. *Journal of Forensic & Investigative Accounting*, **8**, 36-48.

[22] Chen, S.-L., Chen, Y.-Y. and Hsu, C. (2014) A New Approach to Integrate Internet-of-Things and Software-as-a-Service Model for Logistic Systems: A Case Study. *Sensors*, **14**, 6144-6164. https://doi.org/10.3390/s140406144

[23] Nayak, U. and Rao, U.H. (2014) The InfoSec Handbook: An Introduction to Information Security. Apress, New York.

[24] Kumar, G. (2016) Network Security Attacks and Countermeasures. IGI Global, Hershey.

[25] Larrucea, X., Santamaria, I. and Colomo-Palacios, R. (2019) Assessing Source Code

Vulnerabilities in a Cloud-Based System for Health Systems: OpenNCP. *IET Software*, **13**, 195-202. https://doi.org/10.1049/iet-sen.2018.5294

[26] Ali, M.B., Wood-Harper, T. and Ramlogan, R. (2020) A Framework Strategy to Overcome Trust Issues on Cloud Computing Adoption in Higher Education. In: *Modern Principles, Practices, and Algorithms for Cloud Security*, IGI Global, Hershey, 162-183. https://doi.org/10.4018/978-1-7998-1082-7.ch008

[27] Paquet, C. (2013) Implementing Cisco IOS Network Security. Cisco Press, Indianapolis.

[28] Bays, L.R., *et al*. (2015) Virtual Network Security: Threats, Countermeasures, and Challenges. *Journal of Internet Services and Applications*, **6**, Article No. 1. https://doi.org/10.1186/s13174-014-0015-z

[29] Naveed, M., *et al*. (2014) Inside Job: Understanding and Mitigating the Threat of External Device Mis-Bonding on Android. *ISOC Network and Distributed Computing Security*, San Diego, 23-26 February 2014, 1-14. https://doi.org/10.14722/ndss.2014.23097

[30] Calder, A. and Watkins, S. (2010) Threats and Vulnerabilities. In: Calder, A. and Watkins, S.G., Eds., *Information Security Risk Management for ISO*27001/*ISO* 27002, IT Governance Publishing, Cambridgeshire, 110-117.

[31] Calder, A. and Watkins, S.G. (2010) Information Security Risk Management for ISO27001/ISO27002. IT Governance Ltd., Cambridgeshire.

[32] Talabis, M. and Martin, J. (2012) Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis. Syngress, Rockland. https://doi.org/10.1016/B978-1-59-749735-0.00004-X

[33] Mahopo, B., Abdullah, H. and Mujinga, M. (2015) A Formal Qualitative Risk Management Approach for IT Security. *Information Security for South Africa*, Johannesburg, 12-13 August 2015, 1-8. https://doi.org/10.1109/ISSA.2015.7335053

[34] CERT OCTAVE (2008). http://www.cert.org/resilience/products-services/octave/index.cfm