A Cyber Risk Assessment Approach to Federated Identity Management Framework Based Digital Healthcare System

Shamsul Huda * , Md. Rezaul Islam , Vinay Naga Vamsi Kottala , Jemal Hussen Abawajy

Posted Date: 26 December 2023

doi: 10.20944/preprints202312.1750.v1

Keywords: Cybersecurity risk for healthcare; Risk Framework and standards; Risk; threat models; risk mitigations

Article

A Cyber Risk Assessment Approach to Federated Identity Management Framework Based Digital Healthcare System

Shamsul Huda [1,*], Md. Rezaul Islam [2,*], Vinay Naga Vamsi Kottala [3] and Jemal Abawajy [4]

[1] School of IT, Deakin University,Melbourne,VIC, Australia; shamsul.huda@deakin.edu.au
[2] BGD e-GOV CIRT (Bangladesh National CERT, ICT Division,Ministry of Post, Telecom and IT, Bangladesh ; rezakuet99@gmail.com
[3] School of IT, Deakin University,Melbourne,VIC, Australia; vinaykottala1@gmail.com
[4] School of IT, Deakin University,Melbourne,VIC, Australia; jemal.abawajy@deakin.edu.au
* Correspondence: rezakuet99@gmail.com; shamsul.huda@deakin.edu.au

Abstract: Integration of Medical Cyber Physical Systems (MCPS) and Internet-of-Medical Devices (IoMT) with conventional hospital networks have facilitated easy and speedy data collection, vertical and horizontal connectedness and collaborations among healthcare providers. Federated identity management (FIM) provides a solution towards the identity management challenge arising from this integration of millions of MCPSs to get personalized care and frictionless experiences for the patients, doctors, and employees. FIM protocols such as OAuth, Security Assertion Markup Language (SAML) are highly susceptible to cyber attacks like theft of barrier token, replay attack, message insertion, and Man-in-Middle attacks. IoMT devices have vulnerabilities in their firmware, operating systems, data encryption, data at store and data transmission. Combined vulnerabilities of FIM framework and IoMT devices creates major cyber risks for the current digital healthcare system. Therefore, a comprehensive and evidenced based cyber risk assessment is an urgent need for a cyber-safe digital health care system that can avoid frequent life threatening situations. This paper proposes a comprehensive and evidenced based cyber risk assessment approach for FIM and IoMT based collaborative digital healthcare systems. The novelty of the proposed approach is that it considers three dimensional vulnerabilities arising from existing IT communication protocols and infrastructure, IoMT and MCPS medical devices, protocols of FIM and their combined impact on hospitals and provides corresponding recommendations of security controls. The proposed approaches combine two industry standards including Cyber Resilience Review (CRR) asset management, NIST SP 800-30 to take advantages of both approaches. We have used a large number of IoMT and MCPS devices from multiple providers for threat modelling and produced evidence based cyber-risks using attack trees and detailed attack sequence diagrams to validate proposed approaches. The corresponding recommendation of security controls will support healthcare professionals and providers significantly for improving both the patient and medical device safety management within the FIM enabled healthcare ecosystem.

Keywords: cybersecurity risk for healthcare; risk Framework and standards; risk; threat models; risk mitigations

0. Introduction

Extreme demand for high-quality health care for patients [1] has encouraged the healthcare industries to adopt Medical Cyber Physical Systems (MCPS) [2] and Internet-of-Medical Devices (IoMT) [3]. Integration of traditional hospital systems with MPCS and IoMT devices and related systems provides unprecedented horizontal and vertical connectedness and collaboration across healthcare service providers [1–3]. IoMTs facilitate easy collection of patients' data such as blood pressure and sugar level, body temperature, heart condition and their variabilities and many other health parameters through wireless communications [2,3].

 doi:10.20944/preprints202312.1750.v1

IoMT devices such as implantable medical device (IMD)- Implantable cardioverter defibrillators (ICDs) [4,5] allow to read patient heart condition and device information and change settings on devices using external care-link patient monitors, readers, transmitters and wireless (Radio frequency (RF) , WLAN, Bluetooh) protocols [4,5] . These also can be connected to central patient care monitoring systems in the nursing stations in hospitals [6]. Information from ICDs can be transmitted remotely (at home or hospital) to provide operational and safety notification to the clinicians [7]. However devices such as Medtronic ICDs do not use encryption for data transmission, no authentication for critical functions for ICDs [8]. This will allow unauthorized modification of ICD parameters and monitoring devices (MyCareLink Monitor, models 24950 and 24952) [4]. Abbott's ICDs [5] can be compromised through the firmware and communication vulnerabilities allowing attackers to modify settings and issue commands to drain the batteries of ICDs or inappropriate pacing/shocks. This type of damage in ICDs will require surgical procedure to replace batteries and can cause death. This allows terrorists to attack the leader of the countries. An example of these vulnerabilities forced US Vice President Dick Cheney to disable wireless features in his implanted pacemaker [9]. Approximately 350,000 devices in the U.S. are affected by the cybersecurity recall [5] .

Federated Identity Management (FIM) is a promising method where collaborating participants in heterogeneous IT environments share resources securely. In FIM based structure, Identity Providers (IdPs) and Service Providers (SPs) involves in a trust structure which is called Circle of Trust(CoT). The CoT built on a business agreement where users all identifiable information are federated at a central location such as the Identity Provider IdPs. The IdPs passes authentication token to SPs and after that SPs provide corresponding resources to the user [10].

Automatic insulin management systems (AIMS) [11] are personal medical devices and can be connected to patient care monitoring systems that can adjust blood sugar level regularly by providing non-stop delivery of insulin and without daily injections. Wireless protocols and management software can be used to control the settings in the AIMS using mobile applications or central management software in the nursing station [11]. AIMS [11] such as Omnipod has security vulnerabilities which provide unauthorized access to the attackers and allow malicious control of insulin delivery through RF communication intercept and man-in-the middle (MITM) attack. Patient care monitoring systems (e.g. GE Clinical Information Central Stations and Telemetry Servers) [12] are used in hospital to automatically monitor and control the multiple patient monitoring devices form central nurse station inside the hospitals which are also connected with the end-point IoT devices attached to the patients via using LAN and wireless networks. However recently security researchers have discovered major vulnerabilities in GE Healthcare Clinical Information Central Stations and Telemetry Servers' operating system (OS) [13] which is known as 'PwnKit' [13] and MDhex [14]. These vulnerability combined with other eavesdropping access allow to use Polkit components in the OS and then attackers can gain root privilege. The attacker can take full control of nurse station, can install backdoor, can generate false alarm and interfere with other devices attached with the patients. Vulnerabilities in the medical devices combined with network, communication and authentication protocol vulnerabilities cause major data breach on health systems [15]. In USA itself, from August 2020 to July 2021, 706 data breach were reported which includes 44,369,781 individuals' private information [16].

MCPS such as surgical robots [17] are remotely used for under-developed rural areas, disaster areas and the battlefield for surgical procedure allowing smooth and feedback-controlled motions for surgeons via a combination of public and private networks [17]. Prof Alexandre Mottrie of the Department of Urology at the OLV Hospital Aalst, Belgium commented that robot-assisted surgical procedures can reduce post-operative complications and re-admissions which reduces overall costs significantly in very busy hospitals with extreme admission for surgery [18]. Many hospitals in remote cities often don't have expert surgeons. Surgical robots can be used in these scenarios by third party expert services. However these robots can be compromised and be taken over for permanent control by the attackers. Then they can be operated in such a way to cause severe damage to the patients by compromising the software, communication surfaces, installation of backdoor and eavesdropping [17,19].

 doi:10.20944/preprints202312.1750.v1

Many hospitals take third party expert services from wide range of service providers [20,21]. Thus hospitals are connected to a wider health care ecosystems for services and resources sharing. Third party providers requires access to the resources in hospitals or one hospital need to access the resources in other hospitals. This new trend have overburdened hospitals due to their proper identity and access management and human resources processes. It also bring new identity and access management (IAM) [22] challenges for hospitals. Healthcare digital echo systems are now adopting federated identity management (FIM) [22] based IAM solutions [20,22] using different platforms based on OAuth, security Assertion Markup Language (SAML) [22,23] and Google AuthSub [22,23] to consolidate disparate users into a single view of all applications, services and resources from many providers.

The IoMT and MCPS integrated networks enable faster communication, remote management of equipments and service sharing, interoperability of infrastructure, sophisticated and automated monitoring/ controlling of patient care systems, provide more mobility in hospitals, improve the quality of care and reduce costs [1–5,11,17]. Adoption of FIM solution [20,22,23] enable disparate IT systems of one hospital to connect with other services providers' smoothly. At the same time, FIM based solution help integrate, manage and scale millions of IoMT and MCPS devices in the existing hospital systems which facilitates high quality personalize care and frictionless services experiences. However, due to the large attack surface, this interconnection of IoMT and MCPS poses severe cyber security risks including privacy and integrity of patients' data. In more critical situations, any integrity violation of data may result in very costly damage to the patients and could result in life threatening situations [4,5] which would be very difficult to recover.

Health professionals are generally not much aware of the vulnerabilities and the impact of the compromise of connected medical devices. According to Kaspersky research, it is observed that one third of clinicians were not able to protect their patients' data at the time of telehealth sessions [4,16]. At the same time, conventional IT technical staff are also not much familiar with the specific details of the vulnerabilities arising from the new generation of medical devices unless it is discovered by the security researchers and published (e.g. vulnerabilities mentioned in [13,14,17]). According to the National Institute of Standards and Technology (NIST) guideline for Information Technology Security Awareness and Training Program (SP 800-50), [24] management staff and employees needs to be trained to have clear understating of potential risks and threats from security vulnerabilities of the systems they are working. The proposed risk assessment program and different artifacts which have been developed in this paper are very important for training and education for healthcare professional which have been presented in throughout the rest of the paper.

In the literature there are several works available for cyber risk assessment of hospital systems with connected IoMT and medical systems. In [25], Ahmed et.al. proposed different metrics to measure the cyber vulnerabilities impact of the healthcare IT systems. In [9], Floyd, Travis and Grieco analysed the data breach pattern in US hospitals and related vulnerabilities in the hospital systems and their implications. In [26], Coppolino, L. and D'Antonio et.al. proposed a cyber-risk assessment for smart hospital that considers IoMTs' system failures, error related to human when operating IoMTs and bring-your own devices (BYOD) for mobile platform compatible applications in a conventional IT systems. In [27], Abouzakhar, Nasser and Jones reviewed the cyber threats in IoMT enabled hospitals and proposed a vulnerability assessment approach. In [28], Kim, Dong-Won and Choi et.al. develop a method of security assessment of IoMT enabled hospitals identifying and evaluating security threats to these devices, then proposed a multi-criteria decision-making framework based on their related risks. In the literature, most of the works considers cyber-threat under an isolated hospitals. However, due to extreme demand of interoperability among the providers in the healthcare ecosystems, conventional hospital systems need to be connected and their subsequent challenges comes when they work on a federated framework. There is an urgent need of a framework that can identify the challenges, vulnerabilities and propose mitigations for a secure inter-operable and inter-connected healthcare

 doi:10.20944/preprints202312.1750.v1

systems. As mentioned above existing works lacks a detailed cyber risk-assessment framework towards this direction. This is the main motivation of this research.

FIM based IAM solution [20,22,23] with integrated IoMT and MCPS are yet not mature enough to handle life threatening scenarios of critical healthcare functions [21] within a federated framework. FIM has limitations in terms of Trust, Privacy, IDP discovery, Attribute-agitation support [20,22,23]. Prior concept of trust among participants makes FIM implantation difficult for health care situations since FIM shares the Identity attributes and but there is no prevention from service providers (SPs) and identity providers (IDPs) from misusing the shared attributes [22]. SAML does not require authentication for binding and has no requirement for message integrity and confidentiality [13,16]. Attacks like Eavesdropping, Theft of barrier token, replay attack, message insertion, message deletion, message modification and Man-in-The-Middle (MITM) attacks can be a part of this SOP1.1 for SAML protocol binding [23]. Existing vulnerabilities in the IoMT and MCPS when exposed to FIM framework; combined vulnerabilities makes the situation worse than ever.

Therefore In this paper we propose a detailed cyber risk assessment approach for collaborated hospitals with connected MCPSs and IoMTs devices within a FIM framework. The proposed approach considers the vulnerabilities of component in three dimensions: vulnerabilities of existing information technology communication protocols and infrastructure, vulnerabilities of IoMT and MCPS medical devices, protocols of FIM and SSO including OAuth, SAML and their combined impact on hospitals. To the best of our knowledge, the proposed models is a first work in hospital cyber-risk assessment areas. The novelty of the proposed approach are presented in the following:

- A novel cyber risk assessment approach has been developed which considers a Federated Identity Management (FIM) framework with connected IoMT and MCPS devices to meet the next generation healthcare demand and enable safe collaboration among service providers.
- A detailed threat modeling of FIM based federated healthcare has been developed that help identify, prevent, detect, respond and recover against cyber threats to the federated healthcare ecosystems by combining two major standards including CRR and NIST.

Proposed risk assessment approaches considers a broader view of FIM and IoMT protocols including perception layer protocols, network layer protocols and application layer protocols for developing the attack models. Then recommends the appropriate security controls to mitigate the risks. The rest of the paper is organized as follows. Section II presents a comprehensive review of existing approaches to cyber threats in smart hospitals. Section III presents the proposed cyber risk assessment approaches including comprehensive analysis of attacks and their mitigation. Section IV discusses evaluation results of risk analysis and mitigation controls. The last section concludes this research and discusses the future works.

1. Related Work

In [29], DONG-WON KIM et. al. analyzed cyber risk for medical device safety only. They constrained on particular Fennigkoh and Smith model that consider medical device critical functions, physical risk (PR) and required maintenance only. But they don't consider protocol vulnerability or information security.

In [30], M. Kintzlinger and N. Nissim discussed some personal medical devices (PMD) along with their threats, attack flow diagram and security mechanisms. This paper lacks considering protocol or overall threats in the healthcare industry.

In [31], Mohammed Zaki et. al. discussed several attacks on medical devices in smart hospital health care systems. Then they devise a solution using next generation firewall (NGFW) only.

In [32], Luigi Coppolino et. al. analyzed top six categories medical devices of eight most important medical assets in smart hospitals as per outlined in ENISA classification. Among the six categories, top most category belongs to Diagnostic and Monitoring equipment. Author devised a SIEM based monitoring approach here to detect anomalous behavior of critical medical devices. Then

 doi:10.20944/preprints202312.1750.v1

correlating them with intelligent feed and acting accordingly to suggest feasible and appropriate recovery solutions.

R. Sreenidhi Ranganayaki et. al. in [33] reviewed several literature that identify and discuss threats and concerns in healthcare systems. This paper focused to manage workflow of patient's data, secure collection, storage and transmission of clinical patient's data, software solution for viewing and processing of diagnostic data. Author also recommended general cyber security solutions like two factor authentication, TLS solution, multi-layer defense system to mitigate cyber threats.

Gomi et. al. in [34] introduced a FIM based delegation model for systems and proposed a delegation framework that have access control solutions in regards of delegation context. Users can manage their own privileges in the framework enable service providers to manage access of entities based on user's delegated privileges using delegation authority. The authority provides delegation of a delegating entity. Also enables authority to authenticate a user and manages name identifiers of a user.

Kamalanathan Kandasamy et. al. in [35] studied five dominant cyber-attacks in Asian Hospitals and healthcare institutions like Trojan, Phishing, Ransomware, Advanced Persistent Threat (APT), Malware- Credential Compromise. This paper maps each attack with corresponding National Institute of standards and technology (NIST) cyber risk framework guidelines. Specially, it prescribes some vulnerability self-assessment questionnaires(VSAQ) and risk self-assessment (RSAQ) questionnaires in order to help organization identify their present situation.

Zhiqiang Wang et. al. in [36] studied medical imaging cyber physical system (MICPS). Medical imaging device threat model and attack vector discussed along with protection mechanism including data encryption storage, network protection, physical safeguard, system hardening, security guidance. Remarkably, this paper evaluated 15 medical products and identified that none of this products fully meets the satisfaction criteria in terms of requirements.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) OCTAVE Allegro, is tool for risk-based information security strategic assessment and planning. This was developed by Carnegie Mellon University's Software Engineering Institute. This is suitable for an organization implements small teams across business units and IT to work together to address the organization's security needs [37]. In the literature, there is a risk assessment guideline "EBIOS" available for Information System management. These framework provide general guideline for risk assessment and lacks more details of how different artifacts such as attack modeling, threat scenarios [38].

CARMEL ELIASH et. al. in [39] studied most critical Intensive Care Unit Medical Device (ICUMD) security and ecosystems. The taxonomy of ICUMD are analyzed details here including ICUMD security threats, vulnerabilities attack building blocks (ABB), that creates the attack path and promotes actors to penetrate the ICUMD. The 16 cyber threats are mapped with 19 ABB's and their attack frequency figured out. However, this paper constrained only with ICU and similar medical devices.

Dharmendra Kumar et. al. in [40] analysed critical information infrastructure (CII) risk model. Here author reiterated that, advanced technology constitutes managing security of amalgamated digital, analog, physical even human components. Such as SCADA, Smart Meter, Smart Hospitals and Cyber Physical System (CPS). The author emphasized here on technical, governance and user level solutions to mitigate cyber threats. Author mentioned technical, governance related and user level gaps and recommended corresponding methodology and best practices to minimize the gaps.

In [41] Z. Zainal Abidin et. al. devised a conceptual model of risk assessment for detecting insider threats of cyber physical system (CPS). Then author discussed Monte Carlo and Markov chain for risk assessment model. This model is simulation based. Logs from server like IDS, IPS or clouds are collected and analysed using tools and techniques. Although to identify insider threats, synthetic dummy logs are used. The author develops here some insider threats behavior and analysed risk using the Monte Carlo model.

In [42], Abouzakhar et. al. reviewed threats and attacks on IoMT devices. A compromised sensor incorporated to patient's device could results to devastating result or even could cost of life. Most

 doi:10.20944/preprints202312.1750.v1

IoT devices uses IPv6, which introduced to fragment big IP packets over Low Power Personal Area Network (6LoWPAN). This 6LoWPAN is vulnerable to denial of service (DoS) attack. This paper lists down significant threats of cloud sider and their countermeasures.

Gia et. al. in [43] presented a 6LoWPAN based cybersecurity framework for IoMT, which is secure and fault tolerant, scalable. In this complete architecture, IoMT medical sensor nodes integrated in 6LoWPAN connects for Bio signal acquisition from analog front end (AFE) devices and stored in a cloud server to the end users.

Feras M. Awaysheh et.al. in [44] proposed a reference model for access control of Hadoop based big data platform. This article [40] proposed a framework that discusses about security control which can be used as a baseline security for data servers. However paper did not accomplish the cyber-risk framework considering all assets of organization and also did not have a complete attack model of the enterprise organization.

2. Proposed methodology

2.1. Proposed risk assessment approach to FIM based hospital framework with IoMT and MCPS

The proposed approach considers a federated Identity Management (FIM) based hospital framework with connected IOMTs and MCPS. Figure 1 presents the FIM based hospital framework. Hospital 1: As shown in Figure 1, the top parts of the upper section presents the IoMT and MCPS which are connected to the hospital LAN through the Edge gateway and then edge gateway are connected to the cloud computing network via the DMZ server. DMZ server and edge gateway sub-networks are properly segmented and segregated by rule-sets to restrict external access to the sensitive IoMT and MCPS devices. On the upper-left side Hospital network is connected with cloud network for data storage and running different application services. DMZ protects Hospital's internal local-are network (LAN) from untrusted traffic from outside. It generally acts as a subnetwork between public internet and private networks. It protects the data and filter traffic on internal networks by providing an extra layer of security using firewalls. Lower section presents how the FIM is implemented. FIM can use either Security Assertion Mark-up Language (SAML) or OAuth [22].

In the bottom section of Figure 1, Service providers and Identity providers are together referred as SAML providers which involved in authentication and authorization during the SAML requests. The identity Providers (IDP) verify and perform the user authentication. Once user logs into identity provider, they will have the access to FIM-enabled applications. Then IDP and SP works together to authenticate and authorise user and grant access to requested system/application. The conversation between Identity Provider (IDP) and service provider (SP) will happen in a message type called SAML assertion which is an XML document which is created by IDP, verified by SP and it contains all the user information which is relevant for that authentication mechanism. Step-by-step FIM communication process with SAML/OAuth supported protocol is described as below:

1. Clinician would like to access for a system/application from Service Provider (SP), it generates SSOlogin.Request which is sent to SP.
2. Then the SP re-sends the SSO login request to Clinician which then send the request to the IDP. Here Clinician's browser acts as a relay agent.
3. the IDP starts a channel with the clinician for credential verification of client directly and verifies the client's identity with the supplied Clinician's username and password.
4. At this stage, there are different version of IDP response, one version is the IDP then sends the signed SAML response to clinician which has the authentication status. In other version, the IDP sends a session ID to the SP using the redirect channel and then SP send SSO.login response to clinician which allows clinician to access the service.
5. Once SP receives the SAML token/session ID either from clinician or from IDP, SP verifies the authorization privileges.
6. SP provider grants clinician the access to requested service.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1750.v1

7. At last, clinician is able to access to the system/application/service.

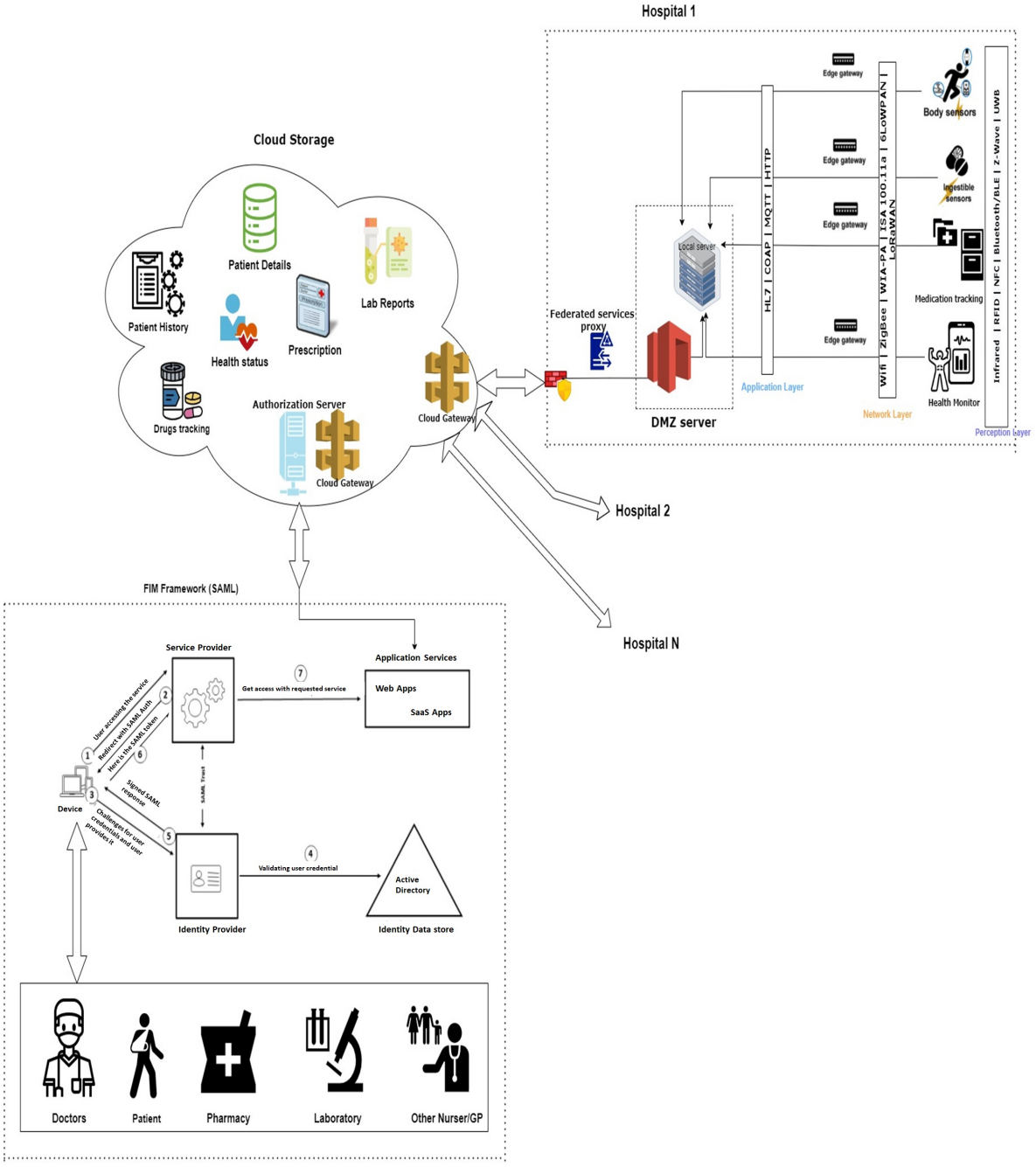

Figure 1. A federated Identity Management based hospital framework with connected IOMTs and MCPS.

The IoMT and MCPS are located in the IoT perception Layer of IEEE 802.15.4. standard. These devices uses protocols like ZigBee, Z-Wave, LowPan, Infrared, RFID, NFC, Ultra-Wideband (UWB). Many of them are also able to connect using WiFi protocol. Devices such as ICDs, Automatic Insulin Management Systems (AIMS), surgical robots, pulse oximeter, blood pressure, temperature sensor, portable EKG sensors and other patient monitoring devices are placed in this layer.

At the network layer, Routers, gateways, access points are located which use IPV6/IPV4, UIP, SLIP, TCP/UDP, 6LoWPAN. Most common application layer protocols are COAP, HTTP, MQTT, HL7

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1750.v1

used in this framework. HL7 is a set of standards that support exchange, sharing, integration and retrieval of electronic health information between health entities is HL7. It defines the packaging and communication details between various exchange systems. In the upper-left section, Cloud Storage is the main subs-systems. At a device layer data are collected from different IoMTs, then stored in cloud database through IoT gateway. The cloud gateway in the cloud storage is responsible for transferring the data from the cloud storage to outside users with the help of authorization server of the FIM framework.

2.2. Details framework of the proposed methodology

The proposed cyber risk assessment approach is based on two approaches including Cyber Resilience Review (CRR) asset management [45], NIST SP 800-30 [46] to take advantage form both approaches. The proposed approach is presented in Figure 2. This involves several stages. At first part of the asset management from CRR [45] is accomplished. If organization is running asset management on a regular basis, then the existing asset profile catalogue can be used directly. This stage involves primarily includes identification of different types of asset such as people, information, technology assets, facility assets and services. Then it needs to document all information related to the asset including assets' sensitivity, asset location, asset owners and custodians, services and assets mapping based on dependency, existing controls of asset, services and sustained requirements of those [47].

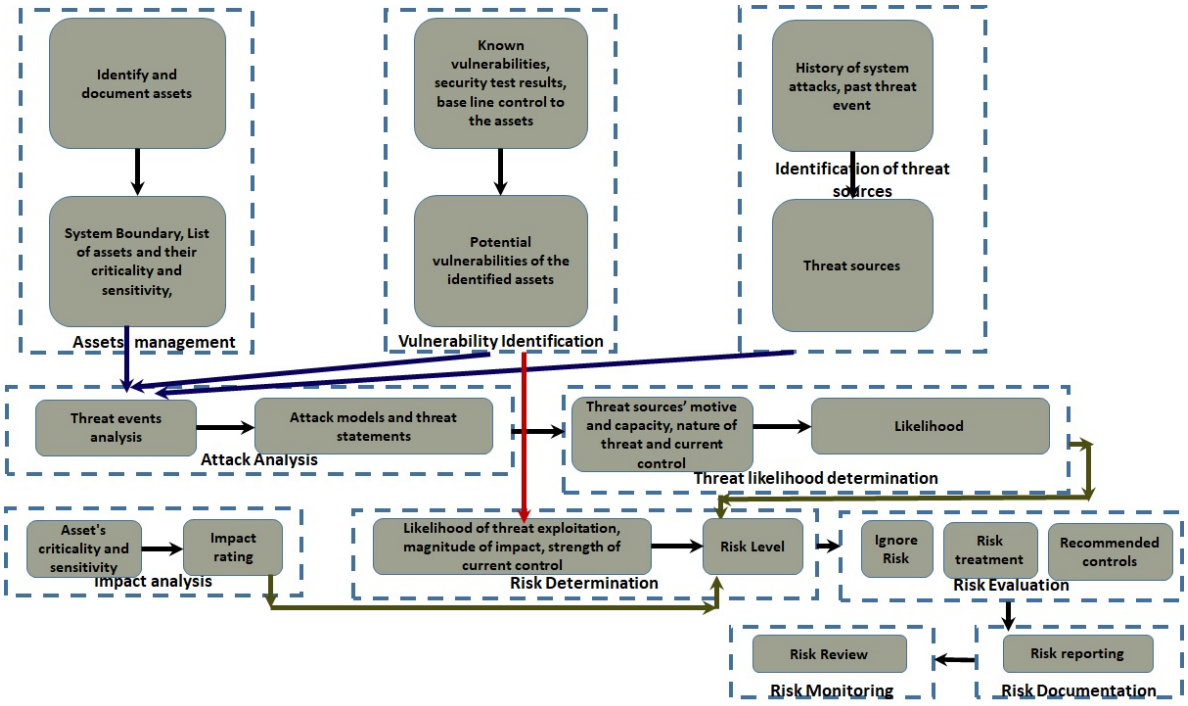

Figure 2. Proposed risk assessment approach to FIM based hospital framework with IoMT and MCPS.

The second step involves identification of the threat sources. The type of threat source can be (i) hostile cyber or physical attacks; (ii) human errors of omission or commission; (iii) structural failures of organization-controlled resources (e.g., hardware, software, environmental controls); and (iv) natural and man-made disasters, accidents, and failures beyond the control of the organization. To determine the threat sources, input values can be assumed by history of the system or threat event (Events which are caused by threat source).

The third steps involve identification of vulnerabilities in the existing assets. These can be identified by gathering known vulnerabilities, security test result and security requirements, by considering these factors we can get the Potential vulnerabilities of the assets.

 doi:10.20944/preprints202312.1750.v1

Fourth step is to develop the attack models. This will develop attack-model statements/threat events by preparing a deeper analysis which combines protocol and assets vulnerabilities together, preparing attack tree and attack sequence graphs based on internal communication of data/data flow, user authentication and data transmission.

Fifth step is to identify the impact of the threat event. The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. The inputs here will be the data sensitivity, data criticality and impact analysis, from these we will identify the impact rating.

The last step is to determine the risk. Risk is a function of the likelihood of a threat event's occurrence and potential adverse impact should the event occur which is calculated from equation-1.

$$Risk = VulnerabilityRating * ImpactRating * Likelihood \tag{1}$$

after determining the risk, we proceed to risk evaluation. There are four options as below:

- Accept the risk: If the likelihood and impact rating is low, the risk is accepted.
- Mitigate the risk: In this case appropriate security control is applied in place to lower the risk level.
- Transferring risk: Risk is transferred to a third party, for example to an insurance company who buys risk as their business [48].
- Risk avoidance: If the risk is extreme high and cannot be mitigated within the current scope of the project, it is avoided.

For asset management and asset catalogue we considered mainly following categories of asset:

- IoMT and MCPS Devices
- Rest of IoT Ecosystem Devices
- Communication related devices
- Infrastructure
- Platform and Backend
- Application and Services
- Information

2.2.1. Threat modeling in the proposed approach for FIM protocols and IoT protocols in federated Hospital

As mentioned in Figure 1, health care staff from different hospitals can access the resources from other hospitals in which the access relationship is many to many. In a FIM framework, main protocols are SAML and OAuth. Both of these protocols have a number of vulnerabilities which make related assets vulnerable. We determine vulnerabilities by attack-sequence diagram analysis.

1.1 Attack sequence analysis for SAML vulnerabilities in hospital's FIM framework SAML vulnerabilities can be exploited when hospital staff using their mobile management systems/applications under FIM framework to access resources in other hospitals/clinics. The clinician login an application using their mobiles which already may have malicious applications installed. This analysis approach has been explained in the sequence diagram Figure 3. As we can see in the Figure 3 either the login credentials or SAML login response with URL are forged by the attacker via the malicious apps in mobile. The attacker can use those to access the resources.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1750.v1

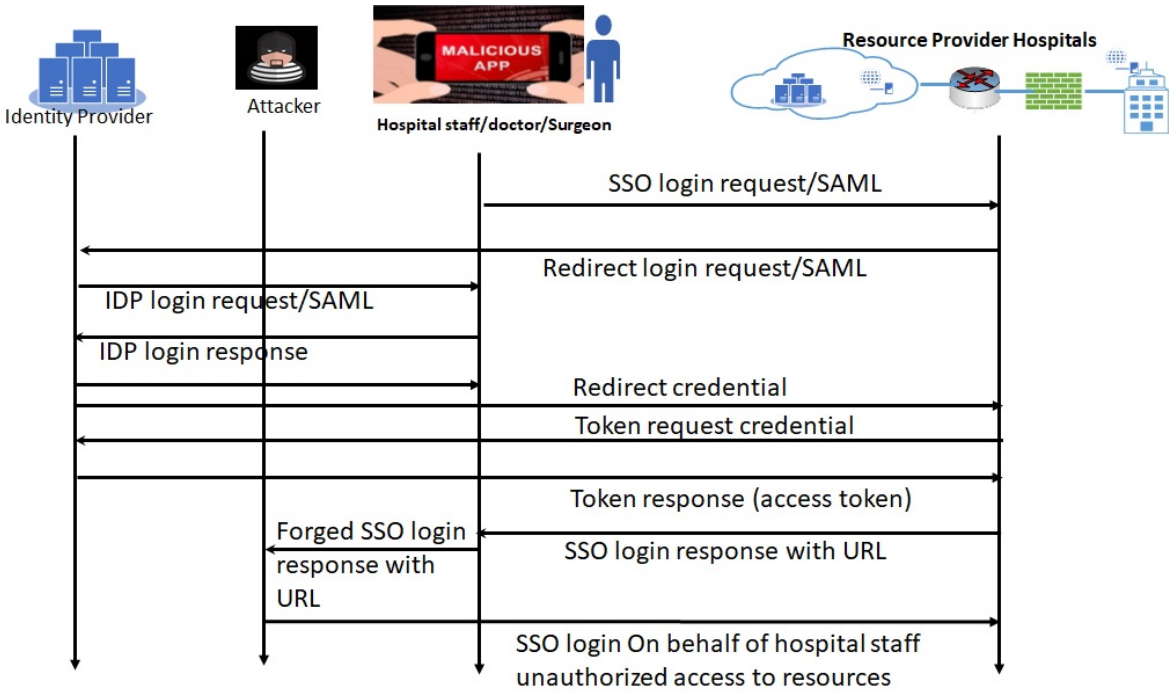

Figure 3. Attack analysis method: An attack sequence diagram when using SAML login into hospital resources.

1.2 Attack sequence analysis for OAuth vulnerabilities in Hospital FIM framework

OAuth vulnerabilities can also be exploited similar to SAML when hospital staff using their mobile management systems/applications. This analysis approach has been explained in the sequence diagram Figure 4. As we can see in the Figure 4, OAuth has a different implementation from SAML, OAuth generated authorization code and then access token. Therefore leaked code or access token which can be used to access the resources by the attackers. There is no authentication process to verify the authorization server in the OAuth. This vulnerability also can be exploited by the same way as mentioned in the sequence diagram Figure 4. Attacker can redirect to any other website and user's credential can be stolen. Later can be used for login into actual authorization server by the attacker. In the implementation of OAuth in the application, if the access token is sent as query parameters in URL, it will be stored in HTTP "referer" and can be accessed by other application and can be used for replay attack. OAuth CSRF bug [49] also can help attackers to get a valid token which can be used to access the login to outlook e-mail account. Similar CSRF attack can be created in FIM based hospital environment.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1750.v1

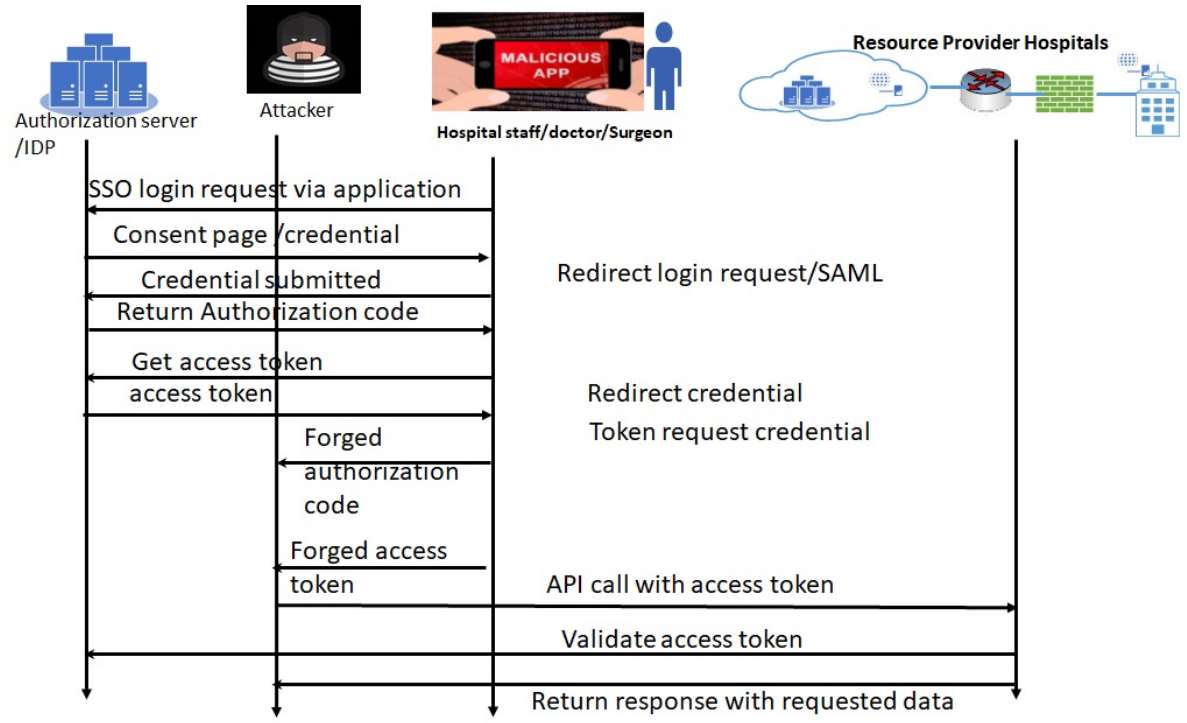

Figure 4. Attack analysis method: An attack sequence diagram when using OAuth based login into hospital resources.

2.2.2. Threat modeling in the proposed approach for perception layer IoT protocols in federated Hospital

IoMT devices such as portable wireless EEG devices (Nihon Kohden airEEG system) are used for long-term routine EEG monitoring and also in ICU environments. Patient monitoring device such as GZ-120 portable patient monitoring are used to monitor Ambulatory Vital Signs including ECG, respiration rate. Several other perception layer devices which carries ambulatory signal such as ECG, EEG, heart are (e.g. NTX/ZM-540/541PA, ZM-530/531PA Nihon Kohden) and corresponding nurse station central monitoring system such as (Nihon Kohden Defensive Monitoring systems) are connected through a number of IoT protocols including Zigbee, z-wave, Wifi, RF as mentioned in Figure 5. These IoMT devices can be compromised by the attackers who are in proximity range of wireless protocols. Physical barrier cannot stop attackers as recent use of drone technologies can overcome the physical barriers. Attackers can use different wireless sniffer (e.g. Wireless CC2531 Sniffer Bare Board Packet Protocol Analyzer Module USB Interface Dongle) in the drone and can come within the proximity of devices. The proposed thereat modeling approach develop the following attack sequence diagrams by theoretical analysis of protocols and device communication behaviour. These are later used for risk determination stage.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1750.v1

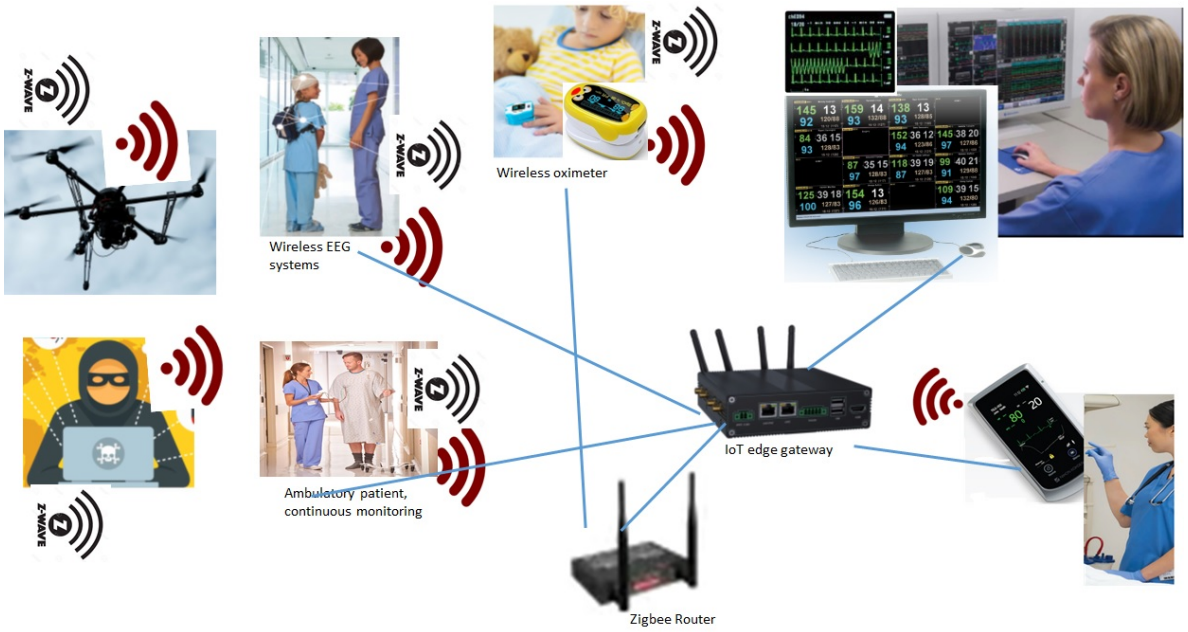

Figure 5. Perception layer devices and their connections with central nurse station in FIM hospital framework via Zigbee, Zwave, wifi and RF protocols.

1.1 Attack sequence for IoMT protocols: Zigbee vulnerabilities in FIM Hospital framework: Figure 6 shows the attack analysis and sequence diagram that can be followed by attacker to disconnect a IoMT device with Zigbee protocol. Attacker runs device scan and then sends identify request inter-pan frame. A factory reset command following this will disconnect the device which can be forced to join in a different (attackers) network. This will allow to access the device information and modification of device setting which can be later left to join the original network and will work as a compromised device in favour of attackers.

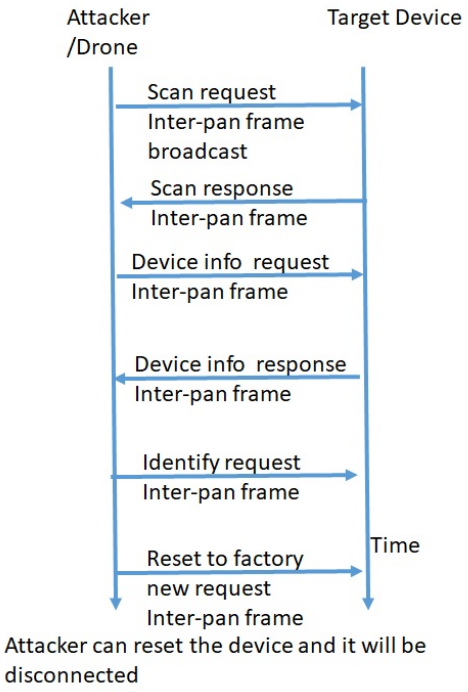

Figure 6. Perception layer devices reset in Zigbee protocol.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1750.v1

Figure 7 shows the attack analysis and sequence diagram that can be followed by attacker to take full control of IoMT devices using Zigbee protocol. Attacker can use Zigbee transceiver (Wireless CC2531 Sniffer) to listen the fresh joining conversation (packets). Often pre-configured link key are published online. Using the pre-configured link key, attacker sends network join end device request with attacker's Network key encrypted using target device's pre-configured link key. Then IoMT device will be joining to attacker's network and fully controlled by attacker. This will allow attacker to get many information from the device. Tampered device can be left to join hospital network again. The same approach can be used to extract hospital network key and then intercept the data, modify the data and send back to teh central nurse station; this is more dangerous and can cause life threatening situations.

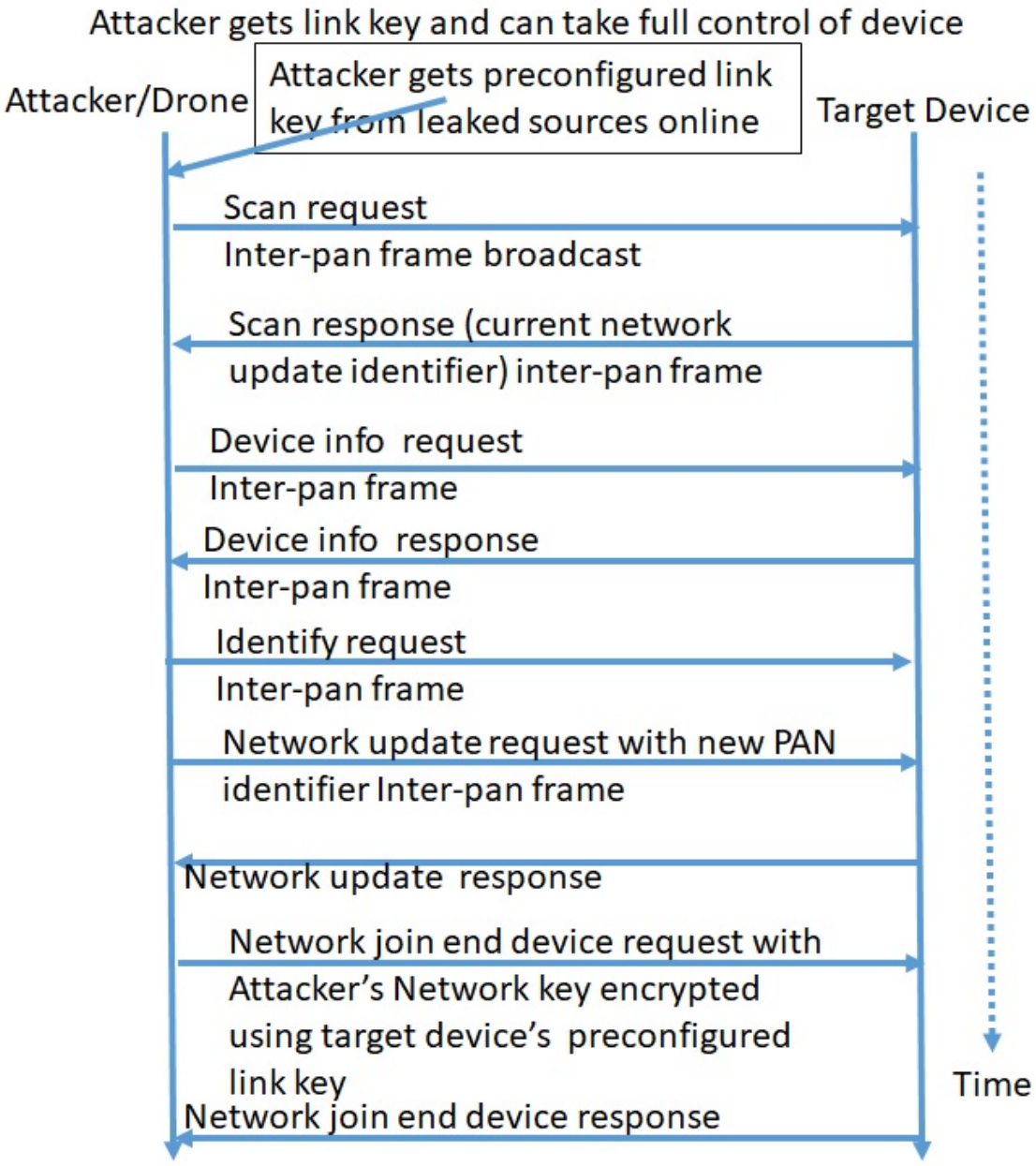

Figure 7. Perception layer devices with Zigbee protocol can be compromised with full control.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1750.v1

Instead of pre-configured link-key, installation code can be used by attacker to take full control of IoMT devices. Figure 8 shows the attack analysis and sequence diagram related to installation code. Attacker gets installation code through dumpster diving. Then attacker calculates the link key using AES Matyas-Meyer-Oseas (MMO) hash function. Attacker starts listening and capturing packets using hardware and IEEE802.15.4 packet sniffer. Then attacker can send network join end device response with encrypted network key using calculated link key from installation code. Then the IoMT device can be taken into attacker network. Attacker can also modify data by extracted network key of hospital (the sniffed packet and installation code generated link key), then send modified data to the central nurse station.

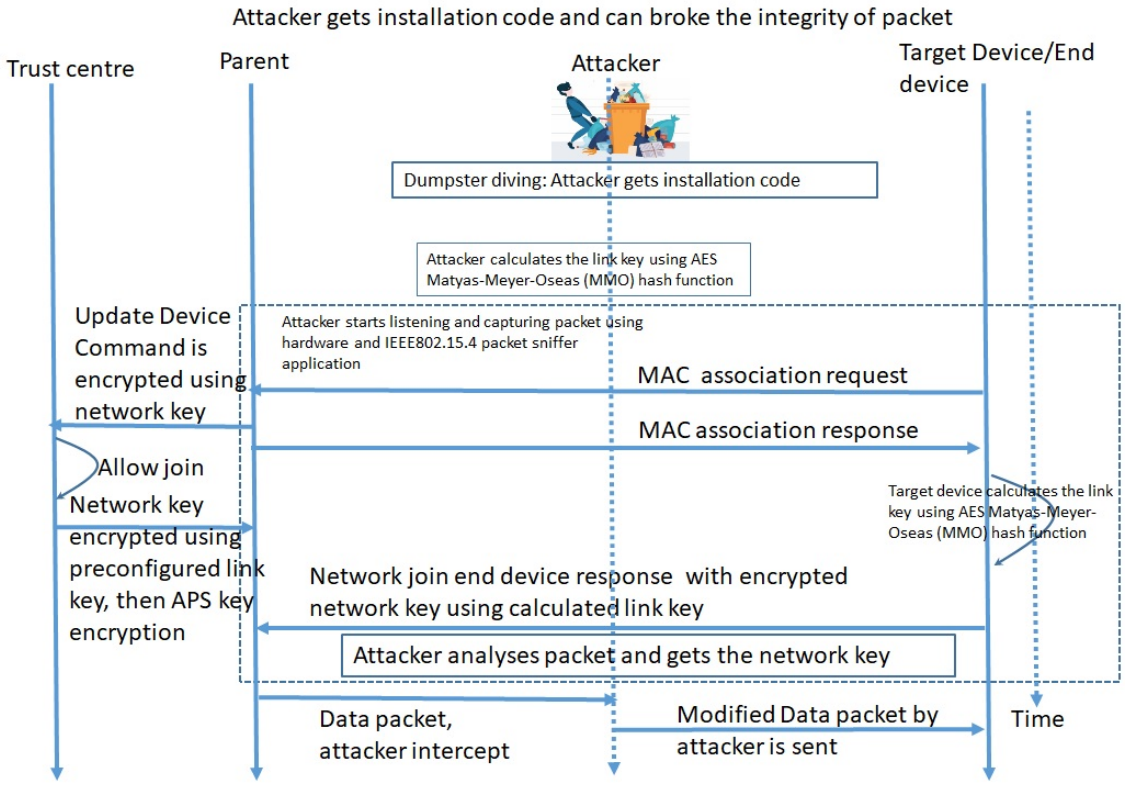

Figure 8. Perception layer devices with Zigbee protocol can be compromised with full control by using installation code.

1.2 Attack sequence for IoMT protocols: WiFi vulnerabilities in FIM Hospital framework: Many of IoMT devices use WiFi protocol to connect to central nurse station or monitoring station. This poses severe security threat to those devices due to known vulnerabilities of WiFi. Attacker continuously scans the SSID and analyze whether SSID visible or hidden, discover the IoMT devices which are connected with Wireless Networks. If wireless device are found in WiFi Networks, then attacker performs password cracking attacks WEP, WPA/WPA2 or LEAP Encryption. Presently, 4-way handshake is used in secured WiFi networks. Among these handshake, the nonce are tricked to reuse the previous key, i.e. reinstalling the already-in-use key. This is called Key Re-installation Attack (KRACK) [50]. In this attack, an attacker forces involved nonce to reset by identifying and replaying re-transmissions of message 3 of the 4-way handshake. As mentioned in the attack sequence in Figure 9, a Pairwise Master Key (PMK) is generated from association and authentication stage between the Supplicant Nonce (SNonce) and Authenticator Nonce (ANonce). In message EAPOL key (Extensible authentication protocol over LAN), ANonce and Unicast message are sent to Supplicant. The Supplicant derive the Pairwise Transient Key (PTK). In message 2 EAPOL key, Supplicant send the SNonce, unicast with Message Integrity Check (MIC). Authenticator derive the PTK and Group

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1750.v1

Temporal Key (GTK), if required. The Authenticator sends ANonce the derived PTK, GTK with MIC to Supplicant message 3 EAPOL key. In message 4 EAPOL key, supplicant sends the confirmation to Authenticator. However, an adversary or attacker in the middle, intercepts and exploits message 4 and bounds both SNonce and ANonce to send further communication through adversary. Meanwhile, thinking that secure communication already established, the supplicant starts sending message encrypted using PTK and adversary exploits the message. Then, adversary tricks both ANonce and SNonce to re-negotiate or re-install the previous PTK. Thus, Once the PTK is extracted, adversary or attacker can modify data sent by the devices at the perception layer to nursing station or vice-versa.

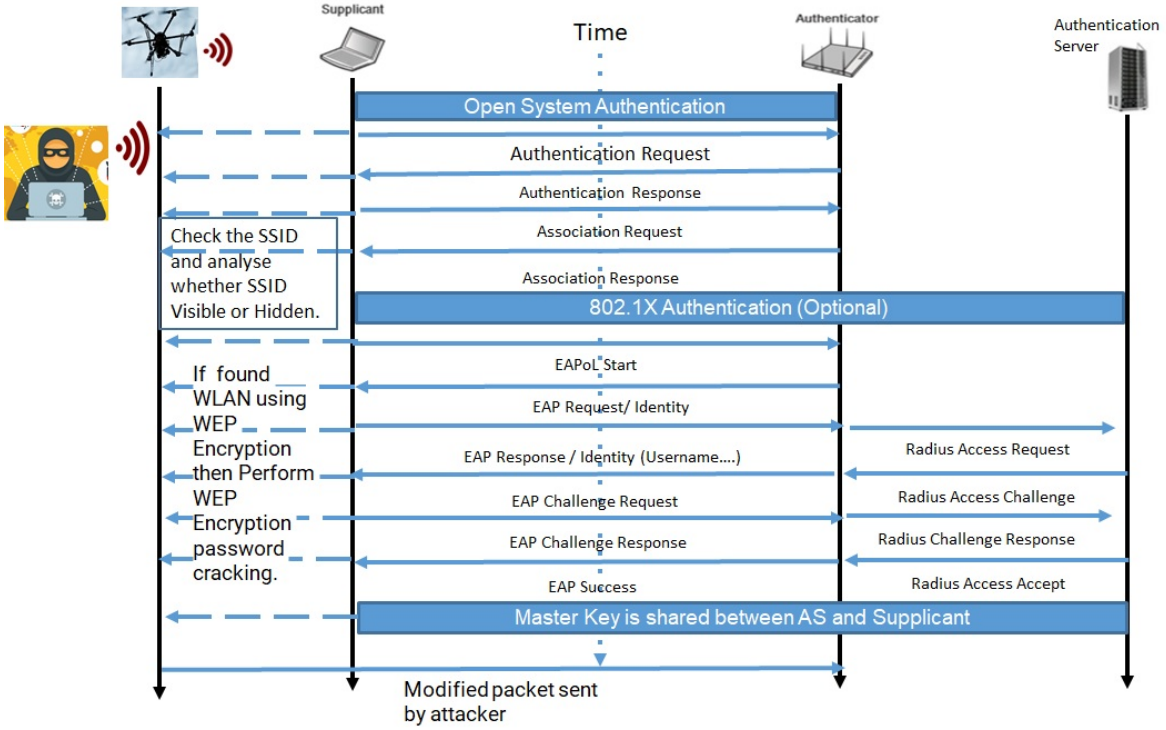

Figure 9. Perception layer devices with WiFi protocol can be compromised by WiFi sniffer.

3. Results and discussion

This study includes IoMT and MCPS devices from several companies including GE healthcare, Ominpod, Nihon Kohden, Abott, Medtronic which considers a large number of equipment's including ICDs,blood pressure, EEG, ECG, patient monitoring devices, central monitoring equipment's in nurse station, insulin pumps. We considered both inside and outside threat sources. A list of threat sources is listed in Figure 10.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1750.v1

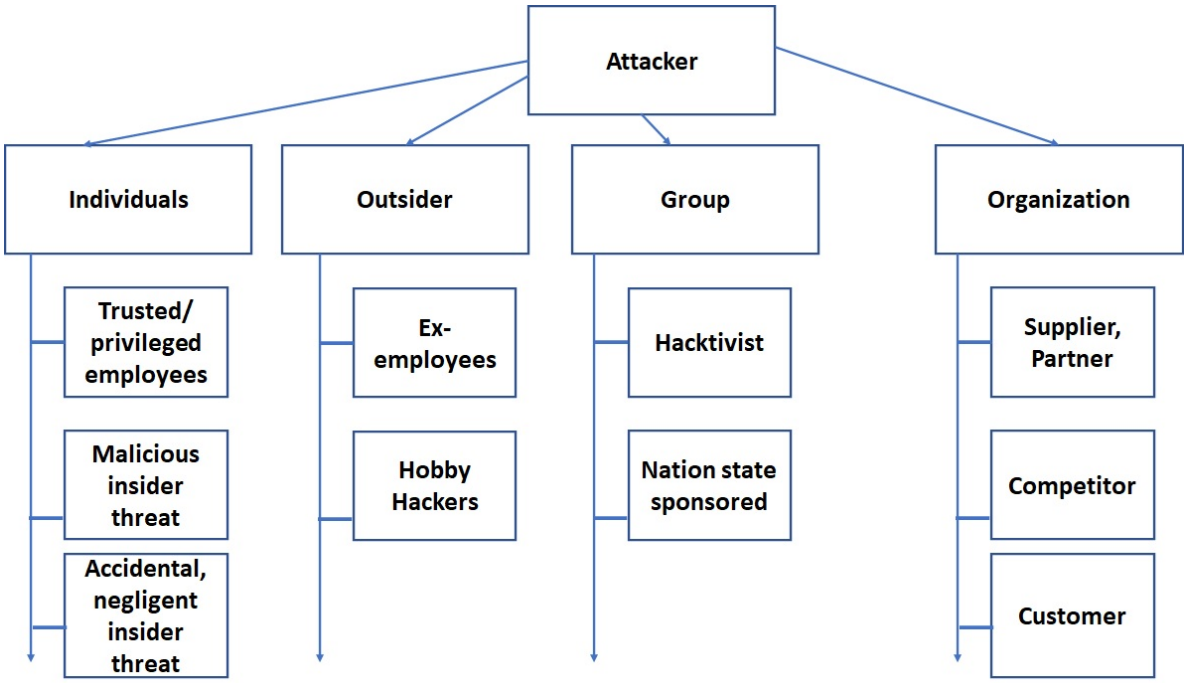

Figure 10. Component of threat model: Identified threat sources.

The threat events in the attacks are identified based on attack analysis in the proposed methodology section. Comprehensive attack sequencing has been accomplished which is then combined and analysed with known protocols and device vulnerabilities to identify detailed threat events for attack models.

Our detailed threat modeling approach derives following attack tree diagrams as mentioned in Figures 11–14 for the attack models by using the attack sequence diagrams for FIM and IoT protocols and related devices according to Figures 3 and 4, 6–9. Each attack is defined by the path of a tree from the root node to a leaf node as shown in Figure 11. The paths in the tree use the sequences of action which are defined in our attack sequence diagrams in Figure 3, 4 and 6–9.

An attack use the event from sequence diagram combined with techniques including Social Engineering, installation of Backdoor at users devices, Brute force attack, Dictionary attacks and Denial of Service Attack (DoS). Attack models in the threat modelling is collection of attacks presented by each path in the tree. Then the attack models are used in risk evaluation.

We calculated cyber risks for the aforementioned IoMT devices which is presented in the following table and also presented the corresponding mitigation strategies column. For privacy reason we have omitted the name companies in the table. However specific vulnerabilities, threat event, attack model and mitigation are directly applicable to those devices which matches corresponding communication protocols and their location in the FIM framework as mentioned in the framework figures: Figure 1 and Figure 5.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1750.v1

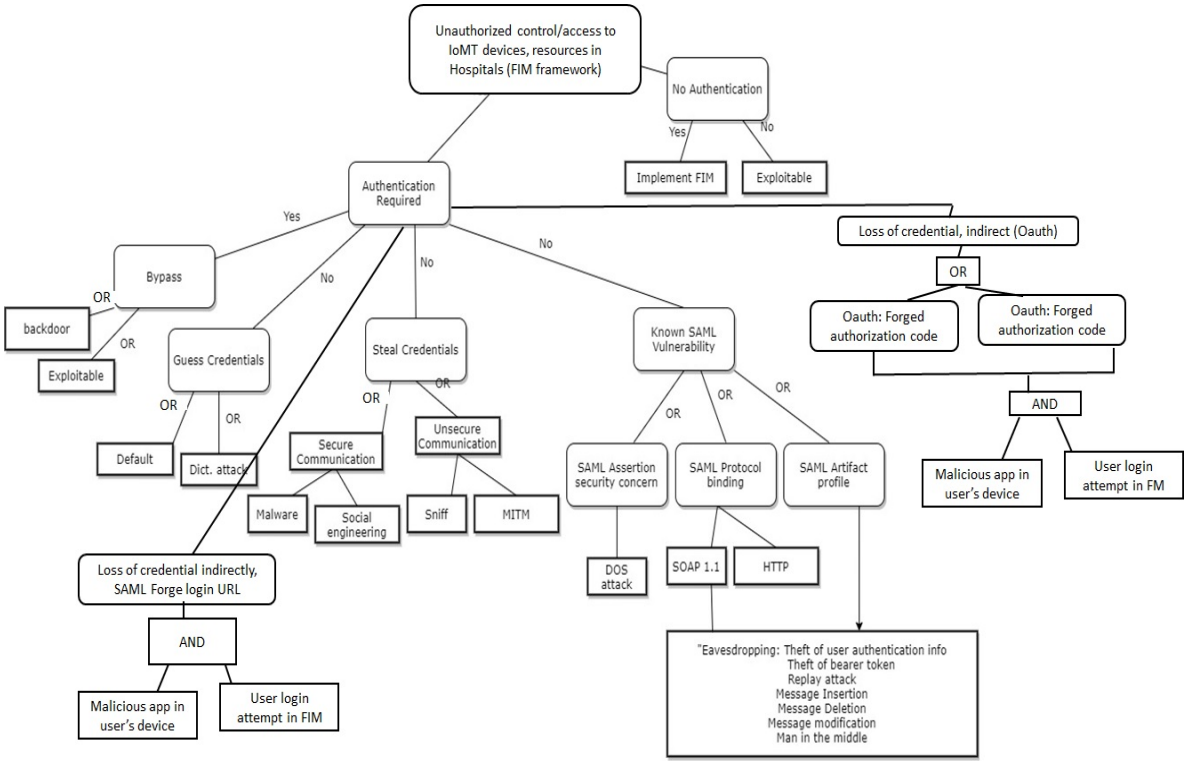

Figure 11. Attack model: Attack tree diagram of FIM framework (SAML and OAuth).

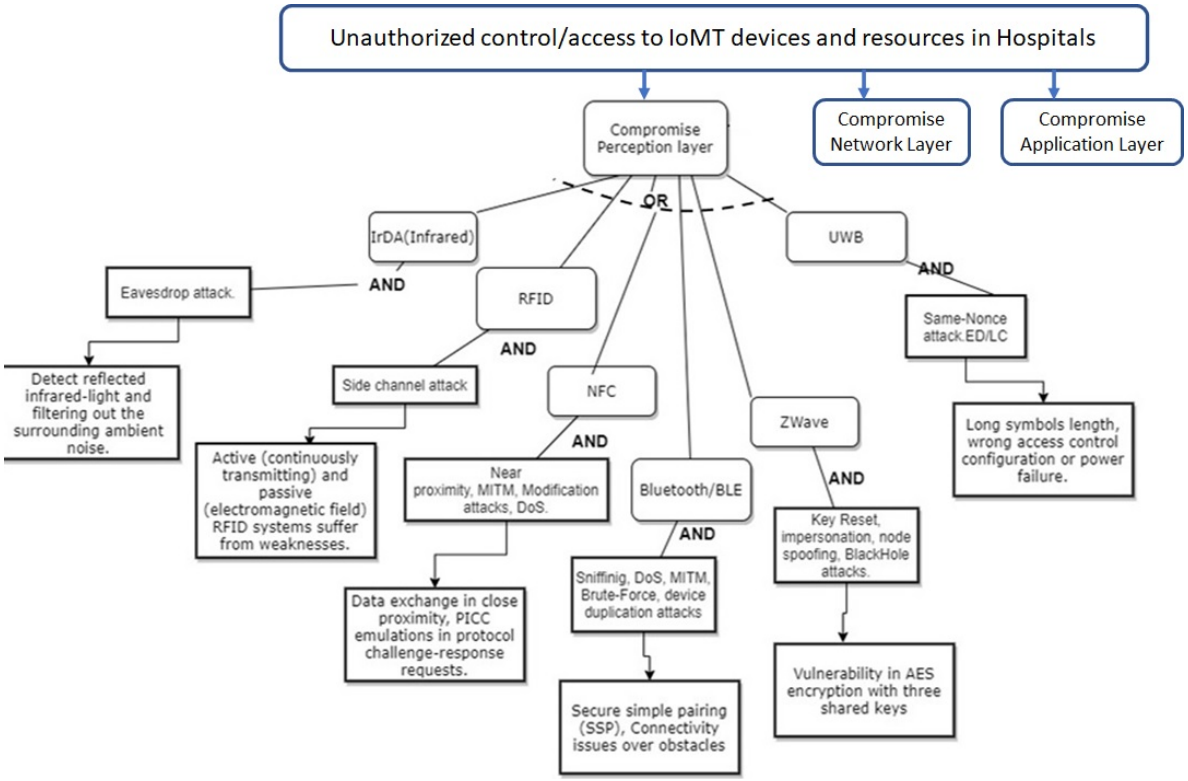

Figure 12. Attack model: Attack tree diagram of IoT protocols (left branch).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1750.v1

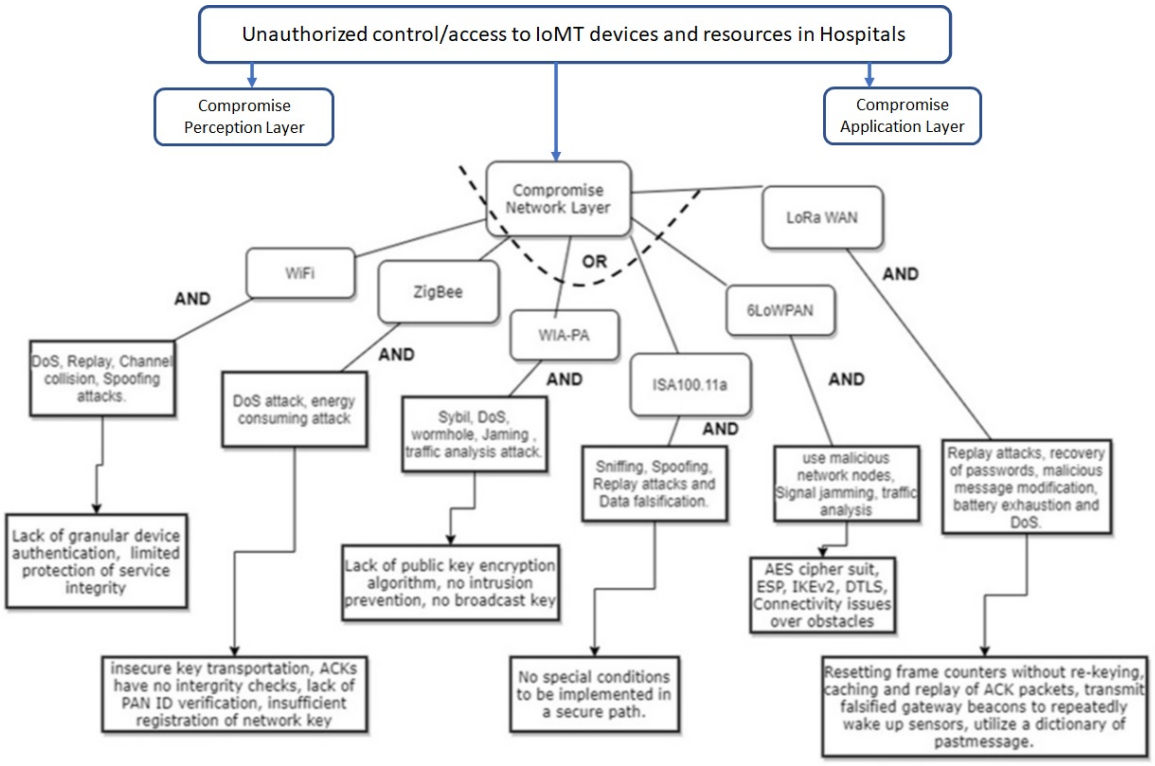

Figure 13. Attack model: Attack tree diagram of IoT protocols (Middle branch), part of Figure 12.

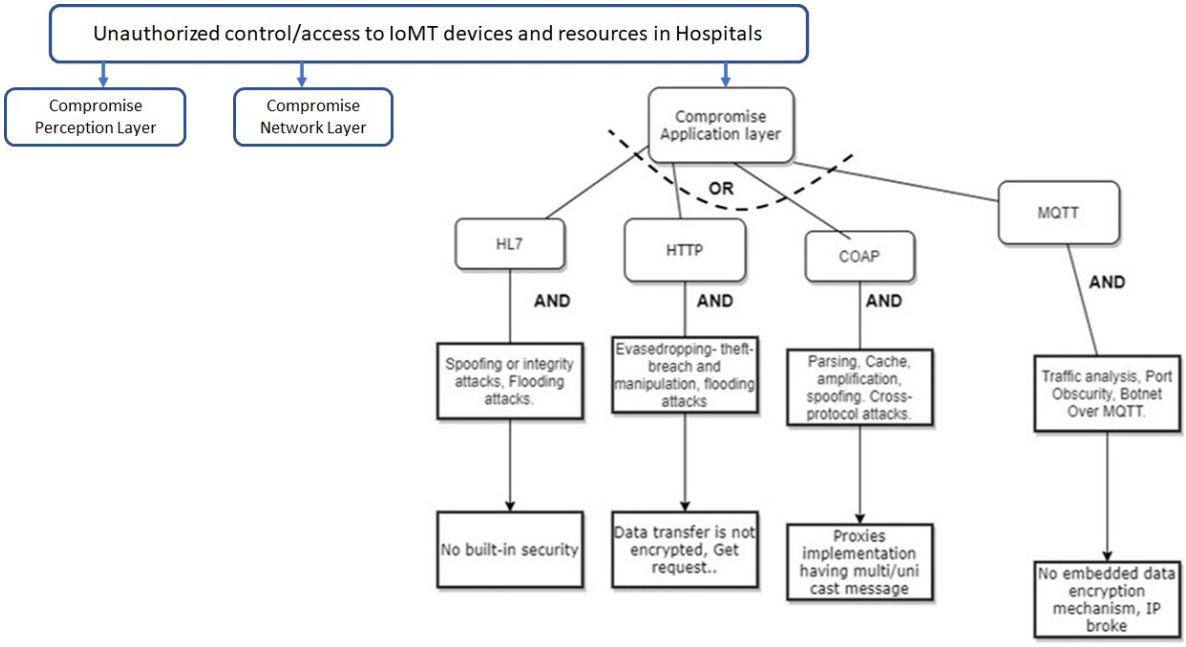

Figure 14. Attack model: Attack tree diagram of IoT protocols (Right branch), part of Figure 12.

3.1. Risk Determination Treatment and Mitigation

Tables II–V present our final risk calculation for MCPS devices. In Tables II–V, all asset groups for IoMT and MCPS infrastructure are considered. Their corresponding weakness and flaws are detailed in these overall IoT asset infrastructure. Then corresponding likelihood, vulnerability rating, level

 doi:10.20944/preprints202312.1750.v1

of impact value are assigned to calculate ultimate risk generated from those individual threats for different assets. The risk value indicates the amount of risk for individual medical IoT devices. Then risk mitigation column in Tables II–V present the required security controls for each type of risks. For IoT devices like actuators, hardware and software, both administrative controls including policies, guidelines and technical controls including monitoring tools (IDS, VAPT) are applicable. Most of the controls are preventive by nature. This will mitigate the risk posed on IoT hardware and software to an acceptable level. For proper risk mitigation in IoT infrastructure section, most technical detective controls are applicable in monitoring and incident response. For threat mitigation in information, network protocol sections, mostly administrative controls are required. Specially, FIM protocol like SAML is authentication and authorization statement protocol among multi-parties. Even if mutual collusion occurs between any two parties, legitimate entities can use validly generated assertion information maliciously. Thus, a trust policy among involved parties, so that parties carry significant liabilities for intentional or inadvertent misuses will mitigate risk. Again, careful consideration should be taken by issuer and re-player about what to put in the assertion, to store assertion in a remote site, which could be exposed to attacker. Moreover, SAML is susceptible to identity forge attack, by which user's identity exposed to attacker. This can be prevented by performing Blockchain for digital identity management, encryption, digital signing i.e TLS encryption and using reputable SAML is a solution. Also following tried and true SAML security best practices [51] will help to mitigate SAML threats accordingly. OAuth risk could be mitigated using Blockchain technology, administrative controls and available technical solutions. Specially, strong security policy enforcement, vulnerability scanning will reduce the risk in OAuth.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1750.v1

Table 1. Assets and their Vulnerabilities.

Asset Group (ID)	Assets	Vulnerabilities in the Assets
IoMT Device (1)	Hardware	**Hardware:** Design Flaw Buffer Overflow Low Processing Power **Software:** 0-day Vulnerabilities Firmware or operating system vulnerabilities **Sensor and actuator:** Weak encryption or no encryption emanations or radiation from devices by visible or non-visible spectrum that causes data leakage Insecure key storage (availability of link-key online availability of installation code) default link key values Unauthorized commissioning
	Software	
	Sensor	
	Actuators	
Other IoT Ecosystem Devices (2)	Devices to interface with things	**Device to interface:** insecure interfaces, Improper IT Assets or business processes design inadequate specifications of IT products, design errors, **Device to manage:** inadequate usability, policy or procedure flows, **Embedded system**:lack of mutual authentication between the client and the server
	Devices to Manage things	
	Embedded System	
Infrastructure (3)	Routers	**Routers:** Buffer overflow, Anonymous proxies, vulnerabilities on the routing path **Gateways:** lack of appropriate segmentation and security architecture, improper segregation **Power supply and Security assets:** Management protocols are not secure, often no encryption.
	Gateways	
	Power Supply	
	Security Assets	
Platform and Backend (4)	Web Based Services	**Web Based Services:** Design Flaw, Buffer overflow complex monitoring due to high traffic gap between service provider, **Cloud Infrastructure:** data owner security control mis-configuration inherently exposed to external access
	Cloud Infrastructure and Services	
Application and Services (5)	Data Analytics and Visualization	**Data Analytics:** Code injection, SQL injection, Path injection, Inference, aggregation **Network and device Management and usages:** Default configuration and password, clear text PDU in management protocol, no encryption in management packet exchange
	Devices and Network Management	
	Device Usages	
Information (6)	Patients' medical record, medical imaging and picture	Lack of proper storage with encryption and poor encryption for data transmission,weak access control
Authentication: FIM framework (SAML): SAML Protocol, SAML Profiles, SAML artefacts, (7)	Client's device (BYOD), Organization device, workstation, Clinician's own workstation and similar devices	SAML binding does not require any authentication , susceptible to all attacks, No authentication and confidentiality requirement for SAML response and assertions, no authentication for service provider to use SAML assertion

 doi:10.20944/preprints202312.1750.v1

Table 1. *Cont.*

Asset Group (ID)	Assets	Vulnerabilities in the Assets
IOT devices: Network protocols, Perception layer, Application layer (8)	Wireless Sensor Network (WSN)	lack of encryption, SNMP agent default community string, Heartbleed bug, Factoring RSA export keys, Lack of Monitoring, insufficient authentication and authorization, poor configuration management, lack of physical security, lack of transport layer encryption, Design Flaw, Buffer overflow, Low Processing Power, default credential, no authentication
	Radio Frequency Identification (RFID) services	
	Web Based Services	
	Cloud Infrastructure and Services	
	Data Mining Application	
	Data Processing and Computing	
FIM framework: Oauth (9)	OAuth protocols and related application software	Lack of proper authentication to verify the authorization server, insecure transmission of query parameters in URI, CSRF bug

 doi:10.20944/preprints202312.1750.v1

Table II. Final Risk Calculation for Federated Identity Management Framework-Based Hospital (IoMT Devices and infrastructure).

Assets	Threat Event	Likelihood	Vulnerability Rating	Impact	Risk	Level of risk	Central patient monitoring devices	IoMT end devices	MCPS (Surgical robots, other MCPS in hospital)	Risk treatment
IoMT Device: Hardware	Unauthorized access to facility Theft, Fraud, Sabotage, Vandalism, Hardware malfunction Supply chain attack "	5	3	9	135	Low	low	low	low	"Applying Physical Control, Proper Control in Supply Chain"
IoMT Device : Software	Access to device software, Alteration of Software, Abuse of 0-day Vulnerabilities"	8	7	9	504	High	High	High	High	Manage and maintain strong password policy, update on patch and technology, Regular Vulnerability Assessment and Penetration Testing (VAPT), Disable unwanted functions Anti-DDoS tool, IPS,IDS installation, Monitoring and Update,
IoMT Device: Sensor	Rating modification, Deletion Supply Chain attack	8	4	8	256	Moderate	Moderate	Moderate	Moderate	Proper Monitoring Proper Control in Supply Chain
IoMT Device: Actuators	Loss of integrity via compromised communication	5	7	7	245	Moderate	Moderate	Moderate	Moderate	"Proper Monitoring Proper Control in Supply Chain"
IoT Ecosystem : Devices to interface with things	Supply Chain attack	5	3	5	75	Very Low	Very Low	Very Low	Very Low	"Message encryption, Anti DDoS, Backup, Proper Control in Supply Chain"
IoT Ecosystem : Devices to Manage things	"Man in the middle Supply Chain attack"	8	3	5	120	Low	Low	Low	Low	"Message encryption, Anti DDoS, Backup, Proper Control in Supply Chain"
IoT Ecosystem : Embedded System	"Eavesdrop attack, Spoofing attacks. Replay attack, Message Deletion Modification, DOS attack"	5	5	9	225	Moderate	Moderate	Moderate	Moderate	"Proper Control in Supply Chain Message encryption"
Infrastructure: Routers	Sniffinig, DoS, MITM, Brute-Force, device duplication attacks.	9	7	9	567	High	High	High	High	Anti-DDoS tool, IPS installation, Monitoring and Update, network segmentation and segregation, appropriate boundary protection, installation of DMZ server and separate critical data assets and critical devices
Infrastructure: Gateways	Key Reset, impersonation, node spoofing, Black Hole attacks.	9	7	9	567	High	High	High	High	Monitoring and Incident response
Infrastructure: Power Supply	ED/LC, Same-Nonce attack.	9	7	8	504	High	High	High	High	Monitoring and Incident response
Infrastructure: Security Assets	Web application attacks , injection attacks (Code injection: SQL, XSS) DoS, DDoS, Replay, Channel collision, Application layer attack i.e. Ping of Death , XDoS, WinNuke , HTTP Floods"	9	9	9	729	Very High	very High	very High	very High	"Anti-DDoS tool, IPS installation, Monitoring and Update"

 doi:10.20944/preprints202312.1750.v1

Table III. Final Risk Calculation for Federated Identity Management Framework based Hospital(Platform and Backend).

Assets	Threat Event	Likelihood	Vulnerability Rating	impact	Risk	Level of risk	Central patient monitoring devices	IoMT end devices	MCPS (Surgical robots, other MCPS in hospital)	Risk treatment
Platform and Backend: Web Based Services	Installing default link keys or sending security headers in clear text on auxiliary frames, logging that causes DoS, euses of Initiation Vectors which may lead to key compromise, energy-consuming attacks.	9	9	9	729	Very High	very High	very High	very High	Anti-DDoS tool, IPS installation, Monitoring and Update, strong remote access mechanism, logging and alert system to targeted server functions, regular scanning and evaluation of interface and code including , proper control for configuration and change management
Platform and Backend: Cloud Infrastructure and Services	Sybil, DoS, wormhole, Jaming , traffic analysis attack.	5	5	9	225	Moderate	Moderate	Moderate	Moderate	IPS installation, Anti-Virus , Malware deployment, Monitoring and Update, Robust configuration/change control, data storage communication encryption, training of system administrators
Application: Data Analytics and Visualization	Replay attacks, recovery of passwords, malicious message modification, battery exhaustion and DoS.	9	5	9	405	Moderate	Moderate	Moderate	Moderate	Message encryption,Anti-DDoS,input validation, output throttling, anonymization
Application: Devices and Network Management	Spoofing or integrity attacks, Flooding attacks, Worms/ Trojans, Rootkits, Elevation of Privileges,	9	5	9	405	Moderate	Moderate	Moderate	Moderate	
Application: Device Usages	Eavesdropping- theft- breach and manipulation, flooding attacks, Abuse of Information Leakage	9	9	9	729	Very High	Very High	Very High	Very High	
Patients' medical record, medical imaging and picture	At Rest: Parsing, Cache, amplification, spoofing. Cross-protocol attacks.	9	9	9	729	Very High	Moderate	low	low	Boundary protection, strong password, Encryption in storage, Antimalware, Port authentication, Log monitoring, Use of SIEM, output throttling system, Tokenization of data, regular backup, Data Loss Prevention (DLP)"
Patients' medical record, medical imaging and picture	In Transit: Traffic analysis, Port Obscurity, sniffing and password cracking in wireless communication, get user detail, installation of backdoor on digital imaging and communications in medicine (DICOM) server	9	9	9	729	Very High	Moderate	low	low	
Patients' medical record, medical imaging and picture	In use: Import of patient data from media storage which has malware embedded, back door installation in this way	8	8	8	512	High	Moderate	low	low	

 doi:10.20944/preprints202312.1750.v1

Table IV. Final Risk Calculation for Federated Identity Management Framework based Hospital (FIM and SAML).

Assets	Threat Event	Likelihood	Vulnerability Rating	Impact	Risk	Level of risk	Central patient monitoring devices	IoMT end devices	MCPS (Surgical robots, other MCPS in hospital)	Risk treatment
FIM SAML: Cleint's device (BYOD), Organization device, workstation,	Eavesdropping: -Theft of user authentication info -Theft of bearer token, malicious app installed in client's device, XMLDSIG's canonicalization algorithms provides weak protection that allow attackers to bypass authentication by creating identical cryptographic signature using XML documents, XML parsing problem can cause incorrect authentication in the SAML assertion"	9	9	9	729	Very High	Very High	Low	Very High	Educate clinicians, monitor the log, alert system, tracking clients, Proper Installation of SAML scanner:SOAP encryption and message integrity, SOAP binding level digital signature, authentication for service provider for SAML assertion and artifacts match, and change management of servers, regular evaluate and asses SAML codes, Mobile device management installed, limit apps installation, Blockchain for digital identity management,managing privacy preferences
FIM SAML: Cleint's device (BYOD), Organization device, workstation,	Replay	2	5	5	50	High	Very High	Low	Very High	
FIM SAML: Cleint's device (BYOD), Organization device, workstation,	Message Insertion	2	5	5	50	Very Low	Very High	Low	Very High	
FIM SAML: Cleint's device (BYOD), Organization device, workstation,	Message Deletion	2	5	5	50	Very Low	Very High	Low	Very High	
FIM SAML: Cleint's device (BYOD), Organization device, workstation,	Message modification	8	8	8	512	High	Very High	Low	Very High	
FIM SAML: Cleint's device (BYOD), Organization device, workstation,	Man in the middle	9	8	10	720	High	Very High	Low	Very High	
IOT devices: Wireless Sensor Network (WSN)	Jamming, Tampering, Exhaustion, Collision, Unfairness	8	8	10	640	High	High	High	High	FHSS,DSSS, Regulated transmitted power, Raising Alarm, Rate Limiting, Error -Correction Code, Small Frames Transmission
IOT devices:Radio Frequency Identification (RFID)	Permanently disable tag, Temporarily disable tag, Replay Attack	7	8	10	560	High	High	High	High	Public-key cryptography Distance Limiting
IOT devices:Web Based Services	DoS, Replay, Channel collision, Spoofing attacks.	5	5	10	250	Moderate	Moderate	Moderate	Moderate	"Public-key cryptography, Strong Password Management, Monitoring, Supply chain Monitoring, Anti malware tool, Port authentication, Network and Application policy enforcement etc."
IOT devices: Cloud Infrastructure and Services	Installing default link keys or sending security headers in clear text on auxiliary frames, Energy-consuming attacks.	5	5	8	200	Moderate	Moderate	Moderate	Moderate	
IOT devices: Data Mining Application	Sybil, DoS, Wormhole, Jaming , Traffic analysis attack.	7	7	7	343	Moderate	Moderate	Moderate	Moderate	
IOT devices: Data Processing and Computing	Use of malicious intermediary network nodes, Signal jamming, traffic analysis, attackers selectively prevent correct packet reassembly.	10	8	10	800	Very High	Very High	Very High	Very High	

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1750.v1

Table V. Final Risk Calculation for Federated Identity Management Framework based Hospital (Oauth related services and applications).

Assets	Threat Event	Likelihood	Vulnerability Rating	Impact	Risk	Level of risk	Central patient monitoring devices	IoMT end devices	MCPS (Surgical robots, other MCPS in hospital)	Risk treatment
Oauth related services and applications	ARP Spoofing, Cache Poisoning, Cross-Site scripting, Man-in-The-Middle (MITM), Drown attack, Denial of Service(DoS) attack, buffer overflow, injection attack, hijacking, Flooding Attacks, EternalBlue attack, trojan horse attacks, shell script attacks, directory harvest attack, Malfunction, Remote Code Execution, Unauthorized Access.	9	9	9	729	Very High	Very High	Very High	Very High	Educate clinicians, monitor the log, use of alert system, tracking of clients location, patching updating of systems, continuous configuration and change management of servers, regular evaluate and asses OAuth interfaces and codes , Mobile device management software installed including device tracking, wiping, policy enforcement, limit apps installation, use tools to verify between code and user, in the implementation redirect-URL should use SSL TLS, use of vulnerability scanner such as OAuth scanner, Perform Blockchain for digital identity management (consider the managing privacy preferences) in healthcare system, Perform industrial IoT Blockchain to secure searchable encryption approach.
Oauth related services and applications	Replay attack	7	7	7	343	Moderate	Very high	Moderate	Very high	
Oauth related services and applications	Message modification	5	5	5	125	Low	Very high	Moderate	Very high	
Oauth related services and applications	Man in the middle, stolen credential	9	9	9	729	Very high	Very high	Moderate	Very high	
Oauth related services and applications	Impersonation attack: Stolen access token, stolen authorization code, malicious app installed, mis-configuration and incorrect implementation of interface in the web application for implicit grant flow and authorization code allows cross-site request forgery (CSRF) and redirection of endpoint to the attackers.	9	9	9	729	Very high	Very high	Moderate	Very high	Educate clinicians, monitor the log, use of alert system, tracking of clients location, patching updating of systems, continuous configuration and change management of servers, regular evaluate and asses OAuth interfaces and codes , Mobile device management software installed including device tracking, wiping, policy enforcement, limit apps installation, use tools to verify between code and user, in the implementation redirect-URL should use SSL/TLS, use of vulnerability scanner such as OAuth scanner, Perform industrial IoT Blockchain to secure searchable encryption approach

4. Future Research Scope

As the pandemic situation emerged, it is obvious to establish smart healthcare system that can monitor patients smartly and efficiently. In the long run, smart SCADA, MCPS, smart meter will be integrated with smart health care system. These items will obviously uncover more vulnerabilities and risk surfaces, but the attacker methods will remain almost same. And the risk assessment including those systems are to be considered in the long run using same methodology depicted in this paper.

5. Conclusions

Medical Cyber Physical Systems (MCPS) have extensively been used in hospital and care providers networks which have enabled collaboration among service providers including management and sharing of resources, remote and automated monitoring/ controlling of patient care systems. However legacy identity management (IAM) solution shows many limitations to this integration. FIM framework reduces administrative overburden of legacy IAM systems, and provide a consolidated single view of data from disparate systems and millions of IoMT and MCPS devices resulting friction-less and streamlined care and services to the patients and healthcare professionals. However, combined vulnerabilities in FIM protocols and IoMT devices brings high operational cyber risk of data breach and life threatening situations. This paper proposes comprehensive cyber risk assessment approaches for FIM based hospital with connected IoMTs. Proposed cyber risk assessment approaches develops detail threat modeling using a combined model from CRR and NIST approaches. The novelty of proposed approach is that it overcome the limitations of existing approaches by applying a three dimensional attack analysis including the ICT infrastructure, FIM protocols and IoT protocols and devices. Proposed approach considers IoMT and MCPS devices from a range of manufacturers including GE healthcare, Ominpod, Nihon Kohden, Abott, Medtronic. Then developed evidenced based thereat model using attack sequence diagrams, attack tree diagrams and risk matrix. Then final risks of MCPS are calculated. The proposed approach successfully identifies threat sources, weakness in the assets and threat events. Finally appropriate security controls for the FIM based hospital networks are indicated. Privacy risk of FIM and its architectural challenge can be considered in an extended version of this paper as a future work.

Author Contributions: Shamsul Huda contributed in conceptualization, methodology, validation, analysis, writing and reviewing. Md. Rezaul contributed in methodology, validation, analysis, writing, Vinay Naga Vamsi Kottala in contributed methodology, validation, analysis, Jemal Abawajy contributed in contributed validation, writing and reviewing.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sun, Y.; Lo, F.P.W.; Lo, B. Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. *IEEE Access* **2019**, *7*, 183339–183355. https://doi.org/10.1109/ACCESS.2019.2960617.
2. Nair, M.; Tyagi, A.; Goyal, R. Medical Cyber Physical Systems and Its Issues. *Procedia Computer Science* **2019**, *165*, 647–655. https://doi.org/10.1016/j.procs.2020.01.059.
3. Razdan, S.; Sharma, S. Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. *IETE Technical Review* **2021**, *0*, 1–14.
4. Food, U.; Administration, D. Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication. https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home.
5. Bryce Alexander, Victor Neira, e.a. Implantable Cardioverter-Defibrillator–Cybersecurity. *Arrhythmia and Electrophysiology* **2020**, *PP*, 1–1.
6. Mersini, P.; Sakkopoulos, E.; Tsakalidis, A. APPification of hospital healthcare and data management using QRcodes. In Proceedings of the IISA 2013. IEEE, 2013, pp. 1–6.

7. Crossley, G.H.; Boyle, A.; Vitense, H.; Chang, Y.; Mead, R.H.; Investigators, C. The CONNECT (Clinical Evaluation of Remote Notification to Reduce Time to Clinical Decision) trial: the value of wireless remote monitoring with automatic clinician alerts. *Journal of the American College of Cardiology* **2011**, *57*, 1181–1189.
8. Das, S.; Siroky, G.P.; Lee, S.; Mehta, D.; Suri, R. Cybersecurity: the need for data and patient safety with cardiac implantable electronic devices. *Heart Rhythm* **2021**, *18*, 473–481.
9. Floyd, T.; Grieco, M.; Reid, E. Mining hospital data breach records: Cyber threats to U.S. hospitals. 09 2016, pp. 43–48. https://doi.org/10.1109/ISI.2016.7745441.
10. Bhargav-Spantzel, A.; Squicciarini, A.C.; Bertino, E. Establishing and protecting digital identity in federation systems. In Proceedings of the Proceedings of the 2005 workshop on Digital identity management, 2005, pp. 11–19.
11. Omnipod. Omnipod Improper Access Control: Cybersecurity Vulnerability Summary. https://www.omnipod.com/product-security/security-bulletins/march-18-2020.
12. Healthcare, G. CCARESCAPE Central Station. https://www.gehealthcare.com/products/patient-monitoring/patient-monitors/carescape-central-station.
13. Food, U.; Administration, D. Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers: Safety Communication. https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-certain-ge-healthcare-clinical-information-central-stations-and.
14. Zeljka Zorz, Managing Editor, H.N.S. MDhex vulnerabilities open GE Healthcare patient monitoring devices to attackers. https://www.helpnetsecurity.com/2020/01/24/vulnerabilities-patient-monitoring-devices/.
15. Sun, Y.; Lo, F.P.W.; Lo, B. Security and privacy for the internet of medical things enabled healthcare systems: A survey. *IEEE Access* **2019**, *7*, 183339–183355.
16. HIPAA Journal on Aug 23, . July 2021 Healthcare Data Breach Report. https://www.hipaajournal.com/july-2021-healthcare-data-breach-report/.
17. Bonaci, T.; Herron, J.; Yusuf, T.; Yan, J.; Kohno, T.; Chizeck, H.J. To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots, 2015, [arXiv:cs.RO/1504.04339].
18. MOTTRIE, P.A. Current use of robots in clinical practice (inside the body, on the body and outside the body) and 4ts perspective. In Proceedings of the the proceedings of Workshop on Robots in healthcare:a solution or a problem?, 05 2019.
19. Fosch Villaronga, E.; Mahler, T. Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Computer Law and Security Review* **2021**, *41*, 105528. https://doi.org/10.1016/j.clsr.2021.105528.
20. Li M, Yang L, e.a. An Approach for Mitigating Potential Threats in Practical SSO Systems. *Information Security and Cryptology. Inscrypt 2015. Lecture Notes in Computer Science* **2016**, *9589*.
21. Gwizdala, S. Healthcare Digital Ecosystems Hinge on Modern Identity. https://www.forgerock.com/blog/healthcare-digital-ecosystems-hinge-modern-identity.
22. Xie, M.; Huang, W.; Yang, L.; Yang, Y. VOAuth: A solution to protect OAuth against phishing. *Computers in Industry* **2016**, *82*, 151–159. https://doi.org/10.1016/j.compind.2016.06.001.
23. Navas, J.; Beltrán, M. Understanding and mitigating OpenID Connect threats. *Computers and Security* **2019**, *84*. https://doi.org/10.1016/j.cose.2019.03.003.
24. Wilson, M.; Hash, J. Building an Information Technology Security Awareness and Training Program.
25. Ahmed, Y.; Naqvi, S.; Josephs, M. Cybersecurity Metrics for Enhanced Protection of Healthcare IT Systems. 05 2019, pp. 1–9. https://doi.org/10.1109/ISMICT.2019.8744003.
26. Coppolino, L.; D'Antonio, S.; Sgaglione, L.; Magliulo, M.; Pacelli, R. Protecting Critical Business Processes of Smart Hospitals from Cyber Attacks. In Proceedings of the 2019 15th International Conference on Signal-Image Technology and Internet-Based Systems (SITIS), 2019, pp. 363-367, doi:, 11 2019, pp. 363–367.
27. Abouzakhar, N.; Jones, A.; Angelopoulou, O. Internet of Things Security: A Review of Risks and Threats to Healthcare Sector. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, pp. 373-378, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.62., 06 2017, pp. 373–378. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.62.

28. Kim, D.W.; Choi, J.Y.; Han, K.h. Medical Device Safety Management Using Cybersecurity Risk Analysis. *IEEE Access* **2020**, *PP*, 1–1. https://doi.org/10.1109/ACCESS.2020.3003032.
29. Kim, D.W.; Choi, J.Y.; Han, K.H. Medical device safety management using cybersecurity risk analysis. *IEEE Access* **2020**, *8*, 115370–115382.
30. Kintzlinger, M.; Nissim, N. Keep an eye on your personal belongings! The security of personal medical devices and their ecosystems. *Journal of biomedical informatics* **2019**, *95*, 103233.
31. Zaki, M.; Sivakumar, V.; Shrivastava, S.; Gaurav, K. Cybersecurity Framework For Healthcare Industry Using NGFW. In Proceedings of the 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). IEEE, 2021, pp. 196–200.
32. Coppolino, L.; D'Antonio, S.; Romano, L.; Sgaglione, L.; Magliulo, M.; Pacelli, R. Protecting critical business processes of Smart Hospitals from cyber attacks. In Proceedings of the 2019 15th International Conference on Signal-Image Technology and Internet-Based Systems (SITIS). IEEE, 2019, pp. 363–367.
33. Ranganayaki, R.S.; Sreeja, B.; Gandhari, S.; Ranganath, P.T.; Kumar, S. Cyber Security in Smart Hospitals: A Investigational Case Study. In Proceedings of the 2021 10th International Conference on System Modeling and Advancement in Research Trends (SMART). IEEE, 2021, pp. 92–98.
34. Gomi, H.; Hatakeyama, M.; Hosono, S.; Fujita, S. A delegation framework for federated identity management. In Proceedings of the Proceedings of the 2005 workshop on Digital identity management, 2005, pp. 94–103.
35. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. Digital Healthcare-Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST perspectives, and Recommendations. *IEEE Access* **2022**.
36. Wang, Z.; Ma, P.; Zou, X.; Zhang, J.; Yang, T. Security of medical cyber-physical systems: An empirical study on imaging devices. In Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2020, pp. 997–1002.
37. Christopher J. Alberts, Sandra Behrens, R.D.P. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0.
38. ENISA. EBIOS:Expression des Besoins et Identification des Objectifs de Sécurité. https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ebios.html.
39. Eliash, C.; Lazar, I.; Nissim, N. SEC-CU: the security of intensive care unit medical devices and their ecosystems. *IEEE Access* **2020**, *8*, 64193–64224.
40. Kumar, D.; Khan, A.H.; Nayyar, H.; Gupta, V. Cyber Risk Assessment Model for Critical Information Infrastructure. In Proceedings of the 2020 International Conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC). IEEE, 2020, pp. 292–297.
41. Abidin, Z.Z.; Abas, Z.A.; Zakaria, N.A.; Hashim, N.A.; Mardaid, E.; Ahmad, R.; Puvanasvaran, A.P. Conceptual Model of Risk Assessment for Insider Threats Detection. In Proceedings of the 2019 1st International Conference on Electrical, Control and Instrumentation Engineering (ICECIE). IEEE, 2019, pp. 1–6.
42. Abouzakhar, N.S.; Jones, A.; Angelopoulou, O. Internet of things security: A review of risks and threats to healthcare sector. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2017, pp. 373–378.
43. Gia, T.N.; Rahmani, A.M.; Westerlund, T.; Liljeberg, P.; Tenhunen, H. Fault tolerant and scalable IoT-based architecture for health monitoring. In Proceedings of the 2015 IEEE Sensors Applications Symposium (SAS). IEEE, 2015, pp. 1–6.
44. Feras M Awaysheh, Mamoun Alazab, e.a. Next-generation big data federation access control: A reference model. *Future Generation Computer Systems* **2020**, *108*, 726–741.
45. Cybersecurity, T.; Infrastructure Security Agency, U. CRR Supplemental Resource Guide: Volume 1, Asset Management, Version 1.1. https://www.forgerock.com/blog/healthcare-digital-ecosystems-hinge-modern-identity.
46. Ross, R. Special Publication (NIST SP) - 800-30 Rev 1. In Proceedings of the Guide for Conducting Risk Assessments, Special Publication (NIST SP), National Institute of Standards and Technology), 2012, pp. 112–120. https://doi.org/10.1109/LCN.Workshops.2017.72.
47. Aljerf, L. Development of a method for classification of hospitals based on results of the diagnosis-related groups and the principle of case-mix index. *EMHJ-Eastern Mediterranean Health Journal* **2016**, *22*, 327–334.

 doi:10.20944/preprints202312.1750.v1

48. Johansmeyer, T. Cybersecurity Insurance Has a Big Problem. https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem.
49. Jack.. Obtaining Login Tokens for an Outlook, Office or Azure Account. https://whitton.io/articles/obtaining-tokens-outlook-office-azure-account/.
50. Vanhoef, M.; Piessens, F. Key Reinstallation Attacks Breaking WPA2 by forcing nonce reuse, 2017.
51. Li, V. Common Pitfalls Of Custom SAML Implementations, 2020.