Turkish Journal of Computer and Mathematics Education Vol.12 No.13 (2021), 1399-1410

Research Article

Threat Analysis and Mitigation for a Secure Healthcare System

Uday Kiran K[1], Swarnalatha P[2] *

[1] M. Tech, Computer Science Engineering, specialization in Information Security, School of Computer Science and Engineering, VIT University

[2]Associate Professor, School of Computer Science and Engineering, VIT University, Vellore-632014, India.
[1]udaykiran.k2019@vitstudent.ac.in
[2]pswarnalatha@vit.ac.in*

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract:

The adoption of networked medicinal apparatus has been aided by significant advancements and advances in communication networks and biomedicinal technologies. Medicinal apparatus have advanced tremendously in the last half-century as a result of such advancements. The widespread integration of technology and medicinal apparatus, on the other hand, is continuously creating new attack vectors. The attack surface has grown dramatically while some apparatus are not stand-alone apparatus and are now web-linked. Many apparatus in use today were designed and built without security features years ago. The importance of regulatory bodies has become clear in such a situation. Before a device may be sold, it must be validated and accepted by the FDA. EU, on another hand, uses a decentralized approach and Notified Bodies (NB) to ensure aloft levels, protection, and efficiency of medicinal apparatus sold in European Nation. After the unit has passed rigorous standards such as fine producing techniques, a Quality Management System (QMS), marking, remote testing, performance specifications, and sufficient storage, it is ready to be used. A memorandum for compliance, that remains legally permanent paper work specifying so a gadget complies accompanied by relevant EU needs as well as they are sold inside European nation, will be granted. Nonetheless, that advent for network competence inside medicinal apparatus has resulted in a significant rise in security and privacy-related attacks. Current regulations lack a standardized mechanism for determining a single protection, safety, and privacy risk that has an impact on patients' health. This study proposes the ISSP Probability Evaluation Architecture for evaluating device's danger category as well as necessary safety commands in order to close these gaps. It's later applied to a infuse set illustration summary as well as it is tested farther next to compared with the existing level as well as enactment. Then comparing reveals so system offers an cohesive perspective for assessing various forms about device dangers.

Keywords: Medicinal Apparatus, CVSS, FDA, EU, Bayesian theorem, ISSP risk assessment process.

1. INTRODUCTION

Prior to the information era, effective and dependable healthcare practitioners were judged on the qualifications of practitioners and the rigor of administrative controls. The healthcare sector has changed dramatically as a result of recent biomedicinal technology advances. Medicinal apparatus, regardless in health centre or embedded in the patient, are becoming increasingly on-the-air computational capacity, networking. Such web worked systems had revolutionized medicinal care and changed the lives of millions of people. According to a new technical study, a single hospital bed contains nearly 10 to 15 web work medicinal apparatus. However, the growing use of connected medicinal apparatus in healthcare has resulted in severe security breaches, putting patients' well-being and health in jeopardy. Analysts out of academe and companies have been regularly confirmed the existence of privacy flaws in linked medicinal applications, as well as the causes of these flaws. The FDA estimated that software vulnerabilities were exploited in nearly 1,527,311 medicinal apparatus over the last decade[1],[2]. Furthermore, the widespread use of wireless technology in medicinal apparatus increases the risk of DDoS hacks.

The healthcare sector has seen an increase in cybersecurity incidents in recent years. Malicious hackers have stolen millions of records from the systems of major companies including Anthem, Premera Blue Cross, and Excellus. In the healthcare domain, Although, healthiness information reports aren't the objective[3],[4]. Web-authorize thyroxine pump, pacesetter,

Magnetic Resonance Imaging devices, extra medicinal apparatus have emerged as a result of the accretion of IoT automation.

The documentation is arranged in succeeding order. Section 2 discusses about introductory understanding of the European Standards, device groups. Section 3 tells about implementation of proposed framework. Section 4 is about the implementation of the framework. Section 5 is about outcomes obtained after the execution of the risk assessment. Section 7 is about the analysis of the framework. The conclusion is shown in Section 7.

2. LITERATURE SURVEY

MDR is a European Union order/directive which took consequence from April 25, 2017. It took the place of the MDD, which is created as well as implemented years earlier. MDR ensures that medicinal apparatus sold in the EU meet high safety and quality requirements. Unlike the Food and Drug Administration, MDR divides apparatus in 4 categories depending on category laws, expected utilization, victim danger [5]. Medicinal device control in the EU is carried out in a decentralized manner.

- MDR is implemented at the national level in each EU state by the Competent Authority.
- NB: They are in charge of medicinal product quality assurance. Furthermore, these organizations ensure that the machines comply with the MDR.
- EC REP: This serves while a liaison in the middle of European Union administration as well as apparatus producers, conducting practical records/information reviews, udi standards, EUDAMED registration, and knowledge sharing. If the producer does not have a physical presence in Europe, they nominate an EC REP.

Both the FDA and the EU have implemented well-known validation criteria for medicinal apparatus in order to ensure their safety [6]. The following sections address these principles and best practices, as well as their drawbacks.

- ISO 14971: It identifies medicinal device hazards through a product-centric risk management approach.
- IEC 80002: This standard establishes a structure for assessing the cybersecurity threats posed by medicinal apparatus.
- NIST 800-30: This special publication from the National Institute of Standards and Technology (NIST) focuses on offering a method for conducting risk assessments.
- 80001-2-8: IEC 80001-2-8: IEC 80001-2-8: IEC It proposes controls and offers a mechanism for managing security vulnerabilities in networked apparatus**.**

The FDA and MDR control medicinal apparatus using the above-mentioned criteria and a risk-management approach[7],[8]. However, as connected medicinal apparatus have become more widely accepted, security attacks have become more common. It's because there isn't a strategy in place that recognizes the combined effect on security, protection, and secrecy threats on person well-being as well as how to mitigate them.

The FDA in the USA is the solitary for an authoritative body which approves apparatus by confirming the efficacy. They control medicinal apparatus build on the danger they pose to victim when in use [9]. Depending on the level for commands needed for ensuring device's efficacy as well as protection, for each apparatus is assigned to one of three regulatory groups. These groups include the following:

- Class I necessitates wide controls.
- Special and general controls are required for Class II.
- Pre-market approval and general control are required for Class III products.

Risk Level	Range of CVSS	Vulnerability Example
Critical	10	RCE, Buffer Overflows, Fault details.
High	7-9	Redirected DOS.

Medium	4-6	Remote Data Revelation.
Low	1-3	Internal Data Disclosure
Informational	0	Device Type, Protocol Detection.

Table 1: Risk Category.

General controls apply on all medicinal equipment. In position to increase efficacy as well as protection for medicinal apparatus, then Food and Drug Administration may maintain an server of recalls [10],[11] , [12] and [13]. The recalls are significant steps taken by the manufacturer to address system failure. The following is a brief summary of the controls.

- **Basic controls** with which all medicinal apparatus can comply are known as general controls. Illegal, impurity, before-markets messages, Application registry as well as lists, files/documentation, goods producing practices are examples of such controls.
- **Special controls** are used to assess the device's efficiency. Post-market monitoring, pre-market data specifications, consistency criteria, special labelling requirements, and patient registries are among the key provisions.
- **Premarket Approval (PMA)** is the process of evaluating the efficacy and protection of class III apparatus through regulatory and scientific analysis.

3. PROPOSED METHODOLOGY

Due to a rise in medicinal device hijackings, determining Integrated Security Safety Privacy threats and the effect on the client health has never been more critical. For industrial critical infrastructure, a number of unified protection and privacy threat administration systems has suggested. Medicinal apparatus, on the other hand, lack such a technique. Instead, different risk management methods that prioritizes medicinal device protection, privacy, or safety are commonly used. By adapting NIST censorious framework recommendations and implementing National Institute of Standards and Technology top implementation and International Organization for Standards requirements, this study focuses to suggest an ISSP system to medicinal apparatus. The proposed framework's key steps are depicted in Fig 1 and considered in the following modules.

3.1 CHARACTERIZATION OF THE SYSTEM

This phase focuses on defining the medicinal device's intended functions and technical requirements, with a particular prominence on the severely and reactivity of facts and info. Software and communication technology requirements are particularly important in this regard. Publicly accessible databases, such as the FDA's, European Union laws, and seller records, assist in obtaining data regarding a specific apparatus. This phase provides detailed knowledge that will be useful in subsequent phases.

3.2 IDENTIFYING THREATS, HAZARDS AND VULNERABILITIES

Identifying all events that cause risks and dangers is the focus of this phase. It all comes down to intrinsic flaws in software design that can compromise safety as well as privacy. It is broken down in to 2 key methods.

- In earlier step the use of CVSS and CWE to list all security vulnerabilities and threats found in the device's software or user interface. CVSS is a system/product protection vulnerability assessment standard that allocates an results depending on the seriousness of the vulnerability. It’s determined by an variety of elements, as well as the complication of the attack, the capability of the threat agent, and the effect on Confidentiality, Integrity, and Availability (CIA). Commom Weakness Enumeration compiles an catalogue of popular safety bugs which focuses on improving instruments to detect, correct, stop them. The probability of exploit is used in this context to assess that if a vulnerability has been found, an opponent with a prequisite advantages can damage it.

- The next step is to use FDA recalls to locate all potentially dangerous incidents that could result in patient harm or privacy violations.

3.3 ANALYSIS OF CONTROLS

Following the discovery of vulnerabilities in medicinal apparatus, it's crucial to examine the obtainable commands which regulate framework need to product acceptance. Critical Digital Assets are the main parts of the structure's probability administration strategy. Critical Digital Assets may ensue equipment, program, precise requirements about the device's security and protection. So, the architecture utilizes the Food and Drug Administration data for checking, the protection and safety controls implemented by such apparatus will be examined. As a result, this system employs controls that are applicable to FDA's medicinal device classes. This system employs Equation 1 to quantify Control Efficiency (CE), or the efficacy of controls implemented in CDA in terms of security and safety.

$$\mathrm{CE(CDA)} = \mathrm{average[CEsafety(CDA), CEsecurity(CDA)]} = +\text{CE serecy (CDA)} \quad (1)$$

where,

• $CE_{security}$ (CDA) are current medical device security measures.

• CE_{safety} (CDA) are current medical device safety controls.

• $CE_{privacy}$ (CDA) are current medical device privacy controls.

Equation 1 will assist in measuring the effectiveness of manufacturer-implemented controls for device approval. Based on the efficacy of the controls, the reliability and well-being correlated commands may possess a value of 1 to 3. Privacy-related access, on the other hand, is a different story. CEprivacy is an binary declaration that has a one or zero output. This step will assist in identifying the safeguards that the system has in place to ensure patient safety.

3.4 DETERMINATION OF VULNERABILITY / THREAT LIKELIHOOD

This phase involves estimating the probability of known internet security susceptibility /menaces affecting the medicinal apparatus in question. By this approach contemplate the effects of a internet security susceptibility on the functionality / efficacy of a medicinal device, as well as the seriousness for client injury. Here it is achieved by looking at the effect of a specific susceptibility on honesty (I), acessibility (A), and victim protection (P) (S). Futher, it considers the impact of a particular vulnerability on patient sensitive data confidentiality (C). It's critical to consider the essence of the susceptibility, risk capability, risk origin motive, present commands when determining vulnerability/threat probability. To assess the threat's probability and magnitude, this method uses one and the other a perceptible and approximate techniques. Where CWE database is consulted in order to determine the threat's probability. It specifies the likelihood of a weakness in terms of its effects.

The proposed solution takes into account the relationship between severity of consequences and the probability of vulnerability/danger, resulting in 4 Risk Levels (TL), with TL4 being extremely excessive and TL1 being very less.

3.5 DETERMINING THE PROBABILITY OF A HAZARD

There are two major methods to calculating hazard probability.

- The Probabilistic hypothesis are used to measure the likelihood of danger phenomenon required to device failure in the initial phase after all the structure put forward a comprehensive proposal to calculating every hazards that could generate well-being danger expected to safety susceptibility, unintended probability, or software malformation.
- The architecture which use these data to calculate the probability of danger based on vulnerabilities and security flaws.

Food and Drug Administration datum callback and studies different various analysis and organizations which is referred as reference to collect data about product failure and patient damage in sequence to measure the probability of a risk. To measure the likelihood of hazard occurrence, this approach integrates conditional probability principles. Equation 2 states that the Probabilistic hypothesis is implemented to measure the phenomenon of danger depending on assorted proof.

$$\mathrm{P(R:SW)} = \frac{\mathrm{P(R)*P(SW:R)}}{\mathrm{P(R)*P(SW:R)+P(R1)*P(EM:R1)+P(R2)*P(U1:R2)}} \quad (2)$$

• P(R) is the likelihood of risk 'R' occurring when programme 'SW' failure.
• P(R1) is the chance that H is electric 'EM' problems occur.

• P(R2) is the likelihood of H where the UI is referred to as a UI. fails to provide precise input or output.
• The likelihood of R due to Software flaws is P(R|SW).
• The likelihood of SW failures if a H occurs is P(SW|R).
• The likelihood of R due to EM is P(R1|EM).
• The likelihood of EM if a R happens is P(EM|R1).
• The likelihood of H due to User Interface flaws is P(R2|UI).
• If a R takes, P(UI|R2) is the likelihood of User Interface failures a location

The likelihood of danger due to any security problem is the second important step in this process. The above-mentioned likelihood of danger which is considered as put in to measure total likelihood, which includes both protection and reliability danger. Equation 3 is used to quantify the frequency of risk 'R' as a result of any threat 'W'.

$$P(R : W) = \frac{P(R) * P(R:W)}{P(W)} \quad (3)$$

• P(R) is the probability of threats where failure of software happens.

• P(R|W) is the probability of threats due to network security susceptibility.

• P(W|R) is the probability of susceptibility if a threat happens.

Because the likelihood utility fall inside the scope 0-1, and 4 main danger phenomenon s aize are explained. Then probability utility that falls between [0, 0.28} is allocated to type I, while the likelihood that falls between [0.25, 0.5) is allocated to type 2. Similarly, likelihood values between intervals [0.5, 0.75) and [0.75, 1) are assigned to levels 3 and 4, respectively. Table I contains a brief overview of each of the allocated levels.

3.6 EVALUATION OF IMPACT

The effect of a threat on person well-being, confidential data, and survival-assisting medicinal equipment is the next critical step. In the proposed framework considers the operation of medicinal equipment, well-being, and the desperation of long-suffering careful info when determining the effect of a threat. Danger effect may be of various levels based on these criteria, as shown in Table II. Controls will be calculated in terms of effect value. The effect of danger on patient health and privacy is a notable concern in this context. As a result, two distinct risk types have been identified: regulated and uncontrolled risk. They each have their own set of treatment, disclose policy. Dangers which have an effect on reliability and protection will be given a total effect digit. Akin dangers carry an uncontrollable probability. These apparatus must execute plan inspection and connected plan of action based on the magnitude of the risk. Managed threats exist, nonetheless, for incidents which had a significant jolt on well-being safety but have a minor effect on well-being privacy. It is critical to run through patches that address vulnerabilities for managed risks. Table II considers the CIA triad to provide a concise overview of the effect of security vulnerabilities on patient safety and privacy.

S.No	Value Of Impact	Confidentiality	Integrity	Availability	Safety of Patient/Client
1	4	Complete or substantial disclosure of therapy data, personal information, and configuration variables conserve in these therapeutic apparatus, its system, or web. As a result, the risk of recognition robbing is huge.	The risk trouper has the ability to change therapy information, personal information, and configuration parameters.	The device and sensitive information would be inaccessible if the threat materialises.	Patient death or permanent injury can occur if the device, its system, or network are unavailable.
2	3	The medicinal device, its framework, or network networks disclose a large amount of therapy data, personal information, and	A threat actor has the ability to change a large number of therapy specifics,	The device's system or network becomes unavailable, resulting in the	The device's, system, or network's inaccessibility can cause disability or

		configuration parameters of an individual.	personal information, and system configuration parameters.	loss of important records, documents, and files.	injury that necessitates medicinal attention.
3	2	Unauthorized knowledge access is impossible since it is limited to the computer or its system.	Changing of a victim's well-being records, treatment configurations, or setting is unlikely, as well as the risk actors has no control over what data is collected.	Significant documents, details, and files stored on the computer or its network become unavailable for a certain interval of hour.	In the event that a computer or network is unavailable, an accident can occur that does not require medicinal attention.
4	1	In the computer, its system, or network, there is no sign of unauthorised entry to PHI, treatment configurations.	Between therapy and configuration environments, therapy information, and patient health information, there is no compromise.	The hazard materialisation results show that there is no output degradation or interruption.	Changes to therapy details or system settings and configurations can cause temporary disruption or disturbance.

Table 2: Value of Impact

3.7 DETERMINATION OF RISK

The most important step in this framework is determining the level of risk. The risk will be calculated based on the effects of the previous measures. Equation 4 will be used to assess the unified well-being and reliability danger of the occurrence specified by a CDA 'd' in a susceptibility 'v' which could be make use of and guide to a threat 'h'.

$$\text{Threat security, safety} = \text{DI}(\text{d}) * \text{HO}(\text{h}, \text{v}) - \text{CE}(\text{d}) \quad (4)$$

Where

- DI stands for the effect of a device's danger on an individual's life.
- HO stands for the combined probability of hazard attributable to common program-correlated problems and privacy threats.
- CE refers to effectiveness of current system commands.

The probability number can be anywhere ranging from one and twelve. As a result, 3 probability category is created, which is shown in Table 3. Equation 5 is used in the standard risk management methodology to measure the probability of data leakage because of security-correlated threats.

$$\text{Threat privacy} = \text{TL} * \text{Impact} - \text{CR}(\text{d}) \quad (5)$$

S.No	Value of Risk	Class of Risk	Explaination
1	0-4	I	Apparatus with a low degree of risk and a need for general protection and security controls.

2	5-8	II	Apparatus which pose a moderate level of danger and necessitate additional reliability and safety measures.
3	9-12	III	Apparatus which pose a high point degree of risk and necessitate imprecise protection and safety controls as well as pre-market approval. There are three subclasses in this class.

Table 3: Different Classes of Medicinal Apparatus

The system allows usage of the Common Weakness Enumeration databases to determine a possible threat which can compromises a patient's privacy or confidentiality. In addition, the Common Vulnerability Scoring Score are used to calculate the effect of a specific vulnerability as well as it's impact on privacy. Subsection III-C discusses power, which is the Boolean formula of security-corelated commands.

3.8 CONTROLS

The unit should have protection and safety commands depending upon the possibility category. Then FDA has also issued comprehensive guidance to normal, specific, and pre-retail acceptance commands in terms of safety controls. Security controls, on the other hand, necessitate the formulation of guidelines. The FDA has proposed guidelines for pre-market clearance that address privacy-associated commands and possibility valuation. But, akin data is insufficient because it lacks a framework for integrating security, protection, and privacy concerns for medicinal apparatus.

3.9 Patch Management and Monitoring

A monitoring mechanism and a patch management system are required depending on the criticality of a computer. All critical device operations will be tracked, and the system will produce an alarm if there is any suspicious activity. Additionally, if the ICS-CERT o reports a cybersecurity vulnerability, manufacturers can apply patches.

4. IMPLEMENTATION OF PROPOSED METHODOLOGY

For assessing possible risks, security vulnerabilities, and ISSP risk worth, the suggested architecture was implemented on infuse pumps. Apparatus category, commands which can be determined based on them in sequence to decrease dangers. The device is used to provide the exact number of medications to the patient.

4.1 CHARACTERIZATION OF THE SYSTEM

These pumps are specifically intended for use in a standby location at the victim's side. Because of advances in biomedicine computing, few inflaters are now compact or can be worn and introduced in Intensive Care Units. To avoid inaccuracies in dose, it is important to administer the medication in a regulated and healthy environment. It is critical to understand the main parts, settings, units, working process of infusion pumps in-order to understand ISSP problems. The following sections go into each of these elements.

- **The infusion pump as a network model**: Admixture pump is not at all lengthy stand-alone apparatus; to load configuration and library settings, the apparatus will commune with the database via wire or wi-fi approach. These settings enable the system to carry out its intended purpose. Pump server keeps track of medicine library, settings in order to work with one another in the healthcare administration method. Then the medicine carriage command and commune subsystems are the two main modules of the pump. The drug delivery controller saves infusion-related data such as dose length, rate, and soon. The communication system govern transmission in the middle of the database, techie, pump's by threat ports such as HTTP, UPNP, Telnet, as well as FTP. The programmer loads settings from the server and infuses them via the drug delivery controller to programmed infusion parameters.
- **Pump programming and configuration settings**: A directory of settings grouped into drug programmers, groups, and profiles can be found in the pump's configurations. The configuration consists of sixteen profiles, each of which contains a batch of side view degree of setting that are farther slitted in 8 types. There are 36 drug services in each of these groups.
- **Pump libraries**: There are two types of libraries for infusion pumps they are regular and fast libraries. The standard library consists of programmes and constraints that can be used to programmed an infusion. To prevent a dangerous situation, it is critical to go through each setting. A fast library, on the other hand, contains medication programmes and predetermined

are crucial to program an infused pump. Those library have protection features, like inaccuracy message if the expounder gives instructions that are outside of the preconceived scale.

- **The Infusion pump workflow and vital details are as follows:** Since infusions come in a variety of delivery modes, a physician can programme medicine manual/instinctively using setup, athenaeum configurations.

4.2 IDENTIFYING VULNERABILITIES, THREATS AND HAZARDS

The previous phase's detailed knowledge about the apparatus's critical unit, assistance, features, system was utilized as an instruction for identifying dangers, risks, threats. Infusions provided through the pump have a 67 percent error rate, according to research. To classify the problems that cause hazards, then the Food and Drug Administration call back from 2006 to July 2019 which were used. This kind of issues are linked to device's programs, as well as charged/machine-like/cell faults and user interface problems. In the FDA's database, there are about 425 recalls and 235 callback (53%) which are due to program errors, where 130 callbacks (32%) were due to voltaic/machine-like, cell non fulfilment problems. Furthermore, 56 recalls were related to UI configuration problems, accounting for 12% on all infused injection flaws. Similarly, publicly documented cybersecurity vulnerabilities are used to identify security vulnerabilities and threats. Incase, the Common Vulnerability Scoring System data file from 2015 to 2019 were considered for identifying certainty flaws which may compromise client privacy and safety.

S.No	Category	Explanation
1	Electrical	Depletion of the battery, Damaged
2	Software	Changes to the drug library, catheter is incorrect.
3	UI (User Interface)	Display that are incorrect.

Table 4: Call back of Infusion Pumps

4.3 ANALYSIS OF CONTROLS

The product under review is a class II device that meets all of the FDA's safety requirements. However, due to the increased risk of adverse effects correlated with the infusion siphon, certain security controls will be included in system. The infusion siphon's specification also lacks privacy-related features. Equation 1 is used to test the controls.

4.4 VULNERABILITY AND THREAT PROBABILITY

This system allows use of the CWE database to assess threat probability. The vulnerabilities recorded between 2014 and 2018 are listed in the previous phase. This process, on the other hand, uses Table VI to define their probability. The overall probability of all vulnerabilities is high, resulting in a TL3 ranking. faraway program code implementation, normal data credentials, meddling, Denial of Services, and improper attestation are five categories that are used to calculate the criticality of vulnerabilities that lead to uncontrolled danger (8). As a result, the total average of unregulated risk is 7.24, while the criticality value of vulnerabilities with managed risk is 6.4.

4.5 DETERMINING THE LIKELIHOOD OF A HAZARD

The threat will be measured twice in this system. The risk of danger is calculated in the first case without taking cybersecurity vulnerabilities into account. As previously mentioned, the infusion pump poses a danger because of 3 major factors: application software glitches, voltaic/machine faults, and UI problems.

The next step is to determine the probability of these risks as a result of cybersecurity vulnerabilities. Such flaws are present in the infusion pump's software and pose a risk. Equation 3 is used to calculate the risk of danger depending on network-security intrusions.

Finally, the probability of danger is calculated by averaging all probabilities, which yields 0.66. According to Table I, the probability of an uncontrolled risk hazard event is level III, which is large. According to CWE, the probability of these managed risk vulnerabilities is large.

4.6 EVALUATION OF IMPACT

This move is critical because it recognizes the effect of a threat on patients' lives. Software-related risks have a major impact on people's lives. The FDA received 56,000 reports indicating a negative effect on human life. About 34% of them said they had suffered life-threatening severe injuries, 68 percent said they had suffered malfunctions and temporary injuries, and 1% said they had died. According to these figures, the seriousness of network reliability intrusions in addition to the effect on persons survival are classified as type 4, which is a quite large.

4.7 DETERMINATION OF RISK

The ISSP risk of medicinal apparatus is calculated in this process. Equation 4 is used to calculate the ISSP possibility of the endue pump using the output from the previous phases.

The CWE database is used to assess the probability of a flaw that compromises a patient's privacy or confidentiality. Furthermore, the impact will be calculated by taking into account the CVSS score of a specific vulnerability as well as it will result on privacy. Command is the Bipartite declaration of solitude-correlated commands, which was previously considered. The probability is peak, in addition to safeguards to be needed to protect the privacy of PHI (Personal Health Information).

4.8 PATCH MANAGEMENT, MONITORING, AND CONTROLS

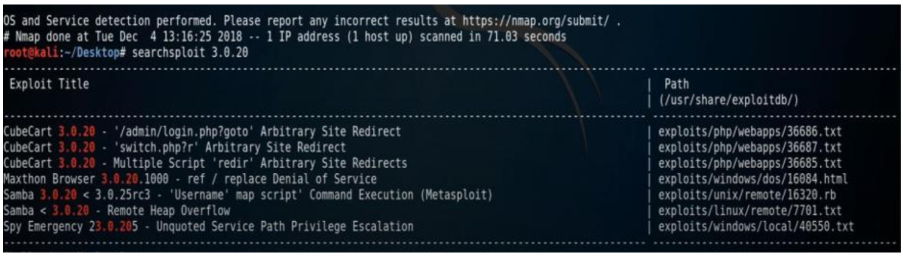
The infusion pump is subject to Category 3 system commands. A proper tracking and audit trail system should be in place. The system should keep track of the pump's transactions in the sequence to find harmful activity in addition to take appropriate steps**.**

5. RESULTS

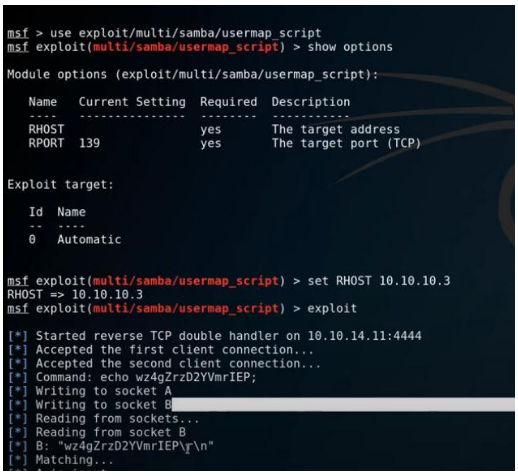
This method consists of execution assessment indicators: threats, security, and mitigation.

(a) Image of the device working accurately before performing attack

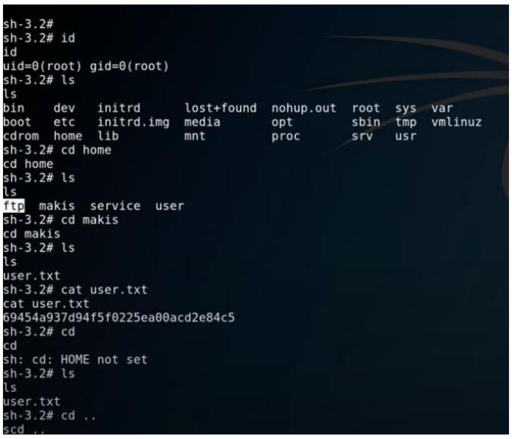
(b) Performing network scan using Nmap to know open ports.



(c) Verifying the Nmap details using searchsploit framework.



(d) Performing exploit to gain system access.



(e) Obtained shell access of the system.

(f) Device values have been modified from 3.0 to 5.0 ml/hr.

6. ANALYSIS

NIST best practices, ISO guidelines, as well as Food and Drug Administration advice papers are compared to the proposed system. The metrics was created to assess the framework's efficacy, as seen in Table 7. The 1st variable programmatic perspective for safety threat evaluation examines the device's safety weaknesses, which have a significant effect on patients' well-being. The comparing of outcome show the suggested Integrated Safety Security Privacy system takes into account, as Table 6 lists every infusion pump flaws and their effect on client security, with the minimum of honesty as well as accessibility. Nonetheless, it is absent from IEC 82304, despite the fact that the FDA's guidelines take these risks into account in part. The 2nd variable is for normal security-correlated flaws that could source system failure or malfunction. The ISSP system uses Food and Drug Administration callback to considered past Software/User Interface problems as well as calculates the likelihood for potential errors affecting victim health using the Bayesian hypothesis, a conditional probability dependent theorem. It's covered in III-E. When comparing these features to current quality, they can be seen by the Food and Drug Administration, International Organization for Standardization 62304, International Electrotechnical Commission 82304, and ISO 14971 all use a threat evaluation approaches to detect flaws in systems, but there is no structured approach to determining the likelihood of danger occurrence. The third and most crucial metric, 'integrated protection and safety evaluation,' measures the combined effect of malicious and non-malicious threats the impact of nature on people's welfare. This is notable since the majority of the researchers accessed and managed their own apparatus maliciously. They were also capable of changing vital settings, which could result in the patient's death. As a result, in this information age, assessing their combined effect is critical.

The suggested architecture tells these issues by calculating merged threat as well as web security effects. In order, infusion pump susceptibilities from Common Vulnerability Scoring System as well as Software/User Interface drawbacks via Food and Drug Administration callbacks were utilized as inputs for assessing non-segregated threat as well as their effects on patients. Nonetheless, Integrated Safety Security Privacy architecture tackles susceptibilities that compromise victim secrecy, as every flaws that affect people's health often affect their privacy, as defined in IV-D. Other main consideration is system categorization as well as commands in terms of protection, as the ISO-62304, IEC 82304, and ISO-14971 specified classes were focused on program failure/User interface. As a result, safety measures were missing. To summarize, the suggested architecture offers a comprehensive perspective to assessing safety, secrecy, as well as ecurity risks, as well as security controls based on device class.

7. CONCLUSION

Security breaches have been increasingly growing since the introduction of internet access in bio-pharmaceutic appliances. The current study suggested an Integrated Safety, Protection, and Privacy menace management system to protect medicinal apparatus. Regulatory bodies' best practices and guidelines are either focused with safety-connected concerns. These bodies place a heavy focus on validating safety-related procedures, ignoring security concerns that have a significant impact on patient health. The proposed structure offers an comprehensive technique for calculating amalgamate protection and reliability dangers, which supports in assessing probability category and required commands for medicinal device security. Furthermore, since most medicinal device manufacturers do not comply with HIPAA legislation, the proposed framework includes a method for calculating privacy-related risks. Future studies should focus on the FDA's review of the new system and its application, as this will aid in the reduction of medicinal device risks.

REFERENCES

[1] M. Joshi, P. Jain and S. P. Mohanty, "Secure-iGLU: A Secure Device for Noninvasive Glucose Measurement and Automatic Insulin Delivery in IoMT Framework," 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2020, pp. 440-445, doi: 10.1109/ISVLSI49217.2020.00-17.

[2] H. N. Qureshi, M. Manalastas, S. M. A. Zaidi, A. Imran and M. O. Al Kalaa, "Service Level Agreements for 5G and Beyond: Overview, Challenges and Enablers of 5G-Healthcare Systems," in IEEE Access, vol. 9, pp. 1044-1061, 2021, doi: 10.1109/ACCESS.2020.3046927.

[3] H. Qiu, M. Qiu, M. Liu and G. Memmi, "Secure Health Data Sharing for Medicinal Cyber-Physical Systems for the Healthcare 4.0," in IEEE Journal of Biomedicinal and Health Informatics, vol. 24, no. 9, pp. 2499-2505, Sept. 2020, doi: 10.1109/JBHI.2020.2973467.

[4] A. Arbelaez, S. Edwards, K. Littlefield, S. Wang and K. Zheng, "Securing Wireless Infusion Pumps," 2018 IEEE Cybersecurity Development (SecDev), 2018, pp. 141-141, doi: 10.1109/SecDev.2018.00037.

[5] S. Jagannathan and A. Sorini, "A cybersecurity risk analysis methodology for medical devices," 2015 IEEE Symposium on Product Compliance Engineering (ISPCE), 2015, pp. 1-6, doi: 10.1109/ISPCE.2015.7138706.

[6] A. Razaque et al., "Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain," in IEEE Access, vol. 7, pp. 168774-168797, 2019, doi: 10.1109/ACCESS.2019.2950849.

[7] A. Arbelaez, S. Edwards, K. Littlefield, S. Wang and K. Zheng, "Securing Wireless Infusion Pumps," 2018 IEEE Cybersecurity Development (SecDev), 2018, pp. 141-141, doi: 10.1109/SecDev.2018.00037.

[8] M. A. Habibi, A. Kusumawardana, S. Wibawanto, H. Wicaksono, Y. D. Mahandi and M. Jiono, "Efficient Electric Water PumpUsing Frequency Based Power Transmission," 2019 International Conference on Electrical, Electronics and Information Engineering (ICEEIE), 2019, pp. 32-36, doi: 10.1109/ICEEIE47180.2019.8981480.

[9] Karthikeyan, T., Sekaran, K., Ranjith, D., Balajee, J.M. (2019) "Personalized Content Extraction and Text Classification Using Effective Web Scraping Techniques", International Journal of Web Portals (IJWP), 11(2), pp.41-52.

[10] T. Javid, M. Faris, H. Beenish and M. Fahad, "Cybersecurity and Data Privacy in the Cloudlet for Preliminary Healthcare Big Data Analytics," 2020 International Conference on Computing and Information Technology (ICCIT-1441), 2020, pp. 1-4, doi: 10.1109/ICCIT-144147971.2020.9213712.

[11] Praveen Sundar, P.V., Ranjith, D., et al. Low power area efficient adaptive FIR filter for hearing aids using distributed arithmetic architecture. Int J Speech Technol 23, 287–296 (2020). https://doi.org/10.1007/s10772-020-09686-y.

[12] P. Ma et al., "A Quantitative Approach for Medical Imaging Device Security Assessment," 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks – Supplemental Volume (DSN-S), 2019, pp. 5-6, doi: 10.1109/DSN-S.2019.00008.

[13] Z. Wang, P. Ma, X. Zou, J. Zhang and T. Yang, "Security of Medical Cyber-physical Systems: An Empirical Study on Imaging Devices," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2020, pp. 997-1002, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162769.

[14] D. Kim, J. Choi and K. Han, "Medical Device Safety Management Using Cybersecurity Risk Analysis," in IEEE Access, vol. 8, pp. 115370-115382, 2020, doi: 10.1109/ACCESS.2020.3003032.