Received: 10 Mar. 2025 | Revised: 25 Mar. 2025 | Accepted: 26 Mar. 2025 | Published online: 25 Apr. 2025

RESEARCH ARTICLE

Journal of Global Humanities and Social Sciences
2025,Vol. 6(3)86-100
DOI: 10.61360/BoniGHSS252017920303

Threat Modeling - Recommendations for a Health Care Facility

Rakesh Ramakrishnan[1,*], Balasubramanian Panneerselvan[2], Prabhagaran Rakkiappan[3] & Manikanta Rudrashetty[4]
[1] *University of the Cumberlands, U.S.A*
[2] *Saveetha Engineering College, India*
[3] *University of Madras, India*
[4] *Procept BioRobotics, U.S.A*

Abstract: Seamless information exchange is crucial in healthcare due to the integration of computational systems. The increased use of Personally Identifiable Information (PII) in digital healthcare raises privacy and security concerns. Threat Modeling Methodologies (TMMs) have emerged to address these challenges by locating and resolving cyber security threats. Early implementation of TMMs equips organizations to combat breaches and understand potential attackers. Integrating techniques, these methodologies strengthen systems and create a comprehensive shield against cyber invasions. However, there is no universal fix for system flaws, necessitating continual adaptation of counter-strategies. Applying threat modeling enables consistent identification, quantification, and assimilation of threats. Determining the most effective approach during product development based on objectives remains challenging. The goal is to scale the chosen strategy effectively, adhere to reporting requirements, and gain valuable insights for enhanced security. This fortifies organizations to navigate the evolving cyber landscape, safeguard PII, and maintain trust.

Keywords: computational systems in healthcare, information exchange, personally identifiable information (PII), digital healthcare,privacy and security threats, health insurance portability and accountability act (HIPAA), threat modeling methodologies (TMMs), integration of multiple methodologies, comprehensive protective shield, system vulnerabilities, adaptable counter-strategies, threats quantification, threat assimilation, threat identifications, safeguarding PII.

Introduction

The transformative power of technology in healthcare has revolutionized various aspects of the industry, ranging from electronic health records (EHRs) and telemedicine to precision medicine and artificial intelligence (AI)-driven diagnostics (Topol, 2019). This digital revolution has opened new horizons for healthcare delivery, facilitating seamless communication, data sharing, and collaboration among healthcare professionals, ultimately leading to improved patient outcomes and population health management (Butcher & Hussain, 2022). This remarkable transformation, although momentous, has been accompanied by potential pitfalls. The pervasive utilization of Personally Identifiable Information (PII) has opened Pandora's box, inadvertently escalating the risk of Privacy and Security Threats. PII encompasses sensitive patient data such as names, addresses, social security numbers, medical history, and financial information, which, if compromised, can have severe consequences for individuals and healthcare organizations (Jusob et al., 2021). With the digitization and interconnectedness of healthcare systems, the volume and complexity of PII have increased exponentially, making it an attractive target for malicious actors seeking to exploit vulnerabilities and gain unauthorized access to valuable data (Wasserman & Wasserman, 2022).

In light of this growing concern, stringent guidelines for the stewardship of PII have been delineated by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA, enacted in 1996 and subsequently enhanced by the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, establishes comprehensive regulations and standards to protect

Corresponding Author: Rakesh Ramakrishnan
University of the Cumberlands, U.S.A
Email: rrakesh711@gmail.com

individually identifiable health information's privacy, security, and integrity (Office for Civil Rights [OCR], 2009). The Act requires healthcare organizations to implement appropriate administrative, physical, and technical safeguards to ensure the confidentiality of patient data and mitigate the risks associated with unauthorized access, disclosure, or alteration of PII (OCR, 2009). A cornerstone of HIPAA compliance is the establishment of robust Access Control mechanisms within computer systems or software applications. Access Control governs the permissions and privileges granted to individuals based on their roles, ensuring that only authorized users can access, view, modify, or transmit sensitive patient information (Zhao et al., 2019). By implementing granular access controls, healthcare organizations can enforce the principle of least privilege, limiting access to patient data to only those who genuinely require it for legitimate purposes, thereby reducing the risk of data breaches and unauthorized disclosures.

However, despite the robust safeguards established by HIPAA, healthcare computational systems remain vulnerable to a broad spectrum of threats. These threats can originate from various sources, including sophisticated cyberattacks, system vulnerabilities, insider threats, and human errors (Gariépy-Saper & Decarie, 2021). Cybersecurity incidents such as ransomware attacks, data breaches, and identity theft have become increasingly common, posing significant risks to the confidentiality, integrity, and availability of healthcare data (Seh et al., 2020). To traverse this precarious landscape effectively, the implementation of Threat Modeling Methodologies (TMMs) emerges as a compelling strategy. Threat modeling involves systematically identifying and evaluating potential threats, assessing their potential impact and likelihood, and devising appropriate mitigation strategies to reduce risk (Martin, 2022). By adopting TMMs, healthcare organizations can proactively identify vulnerabilities, anticipate potential attack vectors, and design robust security controls that align with their unique system architectures and operational requirements (Amini et al., 2015). The early incorporation of TMMs within the developmental lifecycle of healthcare systems is crucial for establishing.

A resilient security posture. By integrating threat modeling activities during the design phase, organizations can identify and address security flaws and vulnerabilities before they manifest in the production environment (Abernathy & Hayes, 2022). This proactive approach enables the implementation of security controls tailored to the system's specific characteristics, ensuring that risks are adequately mitigated, and security objectives are effectively achieved (Alcaraz & Lopez, 2022). Nevertheless, the critical task of selecting an appropriate TMM necessitates a painstakingly in-depth analysis of the product's unique characteristics, combined with an astute choice of methodologies that can encapsulate and neutralize real-world threats pertinent to the product. Organizations must consider system complexity, business requirements, threat landscape, and available resources when determining the most suitable TMMs for their contexts (Umeugo, 2023). It is vital to balance comprehensiveness and practicality, ensuring that the chosen TMMs are sufficiently robust to address the identified threats while remaining feasible and cost-effective to implement (Liu et al., 2012).

Healthcare has undergone a transformation thanks to the seamless integration of computing systems, which has improved patient care, enhanced diagnostics, and operational effectiveness. The potential hazards associated with privacy and security breaches have increased due to the widespread use of PII. Healthcare firms must create robust access control methods to safeguard sensitive patient data and follow strict regulatory criteria, such as those provided by HIPAA, to traverse this environment successfully.

Threat Modeling

How we live, and work has been altered by the seamless integration of computational systems with numerous industries in today's quickly changing, technologically advanced, and innovative world. This integration has brought many advantages to the healthcare industry, where computer technologies have considerably increased patient care, diagnostic accuracy, and operational efficiencies. However, the extensive usage of Personally Identifiable Information (PII) has increased the risks connected with privacy and security breaches, demanding strict procedures to protect sensitive data. As a result, these gains come at a price. Protecting PII becomes essential as businesses rely more on computers to provide healthcare services. Guidelines and strict regulations for processing PII in healthcare settings are established under the Health Insurance Portability and Accountability Act (HIPAA). In addition to being required by law, compliance with HIPAA is crucial for upholding patient confidence and safeguarding the confidentiality and integrity of medical records (Lee & Lee, 2020). HIPAA laws emphasize the relevance of access control measures in computer systems and software applications. The confidentiality, integrity, and availability of PII are protected by access control, which guarantees that only authorized persons have the right amount of access to sensitive patient data. Organizations must take a proactive stance and deploy Threat Modeling Methodologies (TMMs) to combat these threats effectively (Schmeelk, 2019).

A methodical strategy for detecting and reducing potential dangers in software systems is known as threat modeling. The system's architecture must be examined, vulnerabilities must be found, and the possible effects of successful attacks must be evaluated (Malamas et al., 2021). Organizations gain essential insights into potential dangers by adding threat models into the development process, enabling them to decide wisely and devote resources to improve system security. Threat models offer abstractions about possible attackers, exposing their goals and strategies. Organizations can anticipate hazards and create practical countermeasures to reduce them with the use of this knowledge (Viswanathan & J, 2021). Organizations can improve their defenses by discovering vulnerabilities and comprehending potential attack paths, making it much harder for adversaries to take advantage of system flaws. Organizations might integrate numerous TMMs into their current systems to get the best outcomes. A more thorough approach to addressing numerous dangers is provided by the many viewpoints and approaches offered by TMMs (Liu et al., 2012). Organizations can use the benefits and capabilities of each method by integrating various TMMs, improving the system's overall security posture.

Although TMMs are crucial instruments for threat modeling, it's crucial to remember that no single solution can completely eliminate all system hazards. The qualities of the product, the objectives of the company, the available resources, and the degree of knowledge all play a role in selecting the best TMMs. According to (Liu et al., 2012), businesses must carefully assess their requirements and select TMMs that best suit their objectives and resources. Organizations must do a thorough examination of their systems and products in order to successfully use threat models. This examination looks at the architectural design of the product, its design objectives, and the teams' accountability for carrying them out. Organizations can adjust their threat models to handle the unique risks and difficulties associated with their software systems by taking these aspects into account (Martin, 2022). To optimize its effectiveness, threat modeling must be introduced early in the development lifecycle. Organizations can use threat modeling from the very beginning of product design to identify potential hazards and minimize them when doing so is more cost-effective. This proactive strategy lessens the possibility that the system would acquire vulnerabilities during later development stages (European Union Agency for Cybersecurity, 2016).

Beyond risk reduction, threat modeling also provides further benefits. It encourages cooperation among stakeholders from many disciplines while fostering a security-conscious organizational culture. To establish security needs, create suitable controls, and ensure security is a primary focus throughout development, programmers, architects, testers, and security personnel can collaborate (Risk Measures with Applications in Finance and Economics, 2019). An organization's crisis management skills are improved through threat modeling. By predicting potential threats and comprehending their potential consequences, organizations can create incident response plans that are tailored to specific attack scenarios. The ability to respond quickly and efficiently in the event of a security issue allows firms to limit damage and speed up the recovery process (Goniewicz, 2022). Organizations must be diligent regarding their strategies for threat modeling as the threat landscape changes. Threat models are continuously reviewed and improved to ensure their continued applicability and efficiency in combating new threats. To continuously improve their security posture, organizations should keep up with emerging threat trends, industry best practices, and changing regulatory requirements (Luttmer & Samwick, 2018). Standard operations have been revolutionized by the seamless integration of computer systems with numerous sectors. Nevertheless, it has also created new dangers and weaknesses, particularly in terms of security and privacy. Organizations must adhere to regulatory requirements like HIPAA to protect sensitive data and create effective access control systems.

Threat Classes

Let's review some threat classes, class-specific threats related to the Health Industry, and their priorities. (Health Sector Cyber Security Co-ordination Center [HC3] & Department of Health and Human Services [HHS], 2020).

Available Assets

Customers in the healthcare industry can have a wide variety of assets essential for their operations, and such critical assets need protection from external and internal threats. In this section, let's review the generally available assets of a health industry customer (European Union Agency for Cybersecurity, 2016). An integrated network of digital tools makes up the information and communication technology (ICT) ecosystem of a client offering healthcare services. According to (Fichman et al., 2014), the development of digitized healthcare services is exemplified by the complex, symbiotic relationships between various technologies, which range from electronic medical record systems to telemedicine tools and other communication platforms. In a modern hospital setting, the ICT ecosystem essentially acts as the framework and nerve center for the many procedures. The gadgets made to sync with particular software programs are intricately intertwined into the healthcare ICT environment. These highly developed hardware products, which span a variety of medical equipment including blood pressure monitors, glucose meters, and heart rate monitors, are built to establish smooth connection with the software solution. By enabling real-time data gathering and analytical insight, this mutually beneficial relationship closes the gap across technological and the treatment of patients (Furukawa et al., 2010). The communication networks that connect the software being developed and the other gadgets and systems are at the center of this digital coalescence. Through these networks, data flows, allowing the interchange and synthesis of information and transcending the distinction between wired networks like Ethernet and mobile wireless networks like Wi-Fi or mobile phone networks (Zhang et al., 2013).

The advent of advanced ICT ecosystems in healthcare necessitates stringent identity and access management. Identity management systems, which have been proven crucial in safeguarding software product integrity, are entrusted with the dual task of authentication and authorization of users (Jøsang et al., 2007). Authentication, the process of verifying a user's identity, and authorization, the determination of user access rights, are instrumental in ensuring that only authorized individuals can gain access to the software product. This becomes crucial in healthcare settings, where sensitive patient data necessitates stringent security measures. These identity management systems, however, are not merely outside entities. Each software product is furnished with an integrated identity management system. The role of this system is to provide a secure and impenetrable shield for the software product, confining access to the appropriate features and data to authorized users alone (Alshehri et al., 2013). Radio Frequency Identification (RFID) systems operate in concert with the software product. Predominantly used for tracking purposes, these systems serve as the eyes and ears in healthcare settings, tracking everything from equipment and medications to patients. In doing so, they often interact with the software product, perhaps by automatically updating a patient's location in a hospital (Ngai et al., 2008).

The hardware components essential for network connection - the routers, switches, and network interface cards - are the conduits facilitating data transmission and upholding the robustness of network communications. As (Georgakopoulos & Jayaraman, 2016) observed, these pieces of equipment are the pillars supporting the flow of information between devices and the software product over the network. Acting as the gatekeepers to other networks, gateways are vital in routing access to resources. In the context of software products, these gateways channel data requests to appropriate resources, ensuring optimal data transfer while safeguarding the efficiency and security of data transfer (Fu et al., 2018). Engaging with the software product necessitates the use of end-user devices. A wide range of these devices, encompassing personal computers, laptops, smartphones, and tablets, provides the interface for product interaction. By ensuring accessibility and usability, these devices bridge the gap between user and product, thereby contributing to the overall user experience (Wu et al., 2011). The facilities that serve as the physical repositories for the servers and other indispensable resources for product functionality forms the bedrock of the digital healthcare system. These could include data centers or cloud-hosting facilities, but they also extend to the healthcare facilities where the product is being used. In essence, these facilities represent the intersection of digital and physical domains, where healthcare ICT's tangible and intangible elements come together (Jumani et al., 2023).

Table 1

Threat Class I - Authentication

Threat	Priority
Patient Identity Theft – Lost from patient	Low
Patient Identity Theft –Lost from the system	High
Personal Health Record – Compromised from the system server	High

Table 2

Threat Class II – Access Controls

Threat	Priority
Unauthorized Access – System Access through stolen credentials	High
Data Tampering – Unprotected data modification by patients	Medium
Data Tampering – Unprotected data modification by employees	High

Table 3

Threat Class III – Privacy

Threat	Priority
Unauthorized Disclosure – A health care professional discloses patient-related information from the system.	High
Stolen device – A device that can access the patient data is stolen.	Medium
Weak Access Control – Data stored in the patient devices is unprotected.	Medium

Implementing Threat Modeling

Access control is essential to develop a threat model for a product in the Health Care industry. The patient information needs protection from unauthorized access and modification through the threat model. HIPAA defines health providers' production, storage, and transmission of Electronic Protection of Health Information (e-PHI). Such information and its usage have to comply with the retention definitions suggested by HIPAA on health care data. Working with e-PHI on uses, disclosures, modifications, and deletions are defined as the term "Access". Access can either be authorized or unauthorized. Authorized access can be further classified into legitimate authorization or improper authorization. (Alshehri et al., 2013) The Threat Model creation is implemented through the following steps:

Security Goal Setting

Security goal setting is a paramount strategy, entailing the establishment of clear, measurable, and attainable objectives in information security (Mead & Stehney, 2005). As a systematic and proactive approach, it aligns with the overarching business goals while preserving confidentiality, integrity, and availability of the information systems. The trident of security goals comprises protection, detection, and reaction, each interlaced with the other and yet distinctly essential (Mead & Stehney, 2005). Protection goals are centered on the robust safeguarding of systems against potential threats. These objectives prioritize implementing appropriate security measures, encompassing both technical (such as firewalls and encryption) and organizational (like security policies and employee training) mechanisms aimed at thwarting cyber-attacks and unauthorized access (Sokolnikov, 2017). Detection goals, however, revolve around proactively identifying and continually monitoring potential threats and vulnerabilities. The quintessence of these objectives is the real-time detection of anomalous activities and potential breaches, achieved through measures like intrusion detection systems, log monitoring, and security audits (Elmasry, 2019). The third facet of security goals, the reaction goals, concerns the organization's response to security incidents. These objectives underscore the importance of swift, efficient response strategies to contain and mitigate the impact of security breaches. They span a range of activities, from incident response plans and disaster recovery procedures to the legal and communicative actions undertaken post-incident (Mead & Stehney, 2005).

In essence, security goal setting operationalizes the concept of cybersecurity, translating strategic vision into concrete objectives. This process establishes a synergistic link between threat modeling and goal setting, enabling an intricate understanding of the security landscape to inform goal-setting endeavors. Such a comprehensive and forward-looking approach to security provides organizations with the impetus to withstand and thrive in the face of evolving cyber threats. The access policies need to be determined based on the organizations using the product. These policies should comply with the standards of the customer organizations and HIPAA regulations.

System Overview Development

The preliminary functionalities of the system need to be considered while building the Security Threat model. There should be proper communication channels to ensure the accurate and timely flow of information among the entities working with the product.

System Comprehension

Once the data entry and exit locations are identified, a step to define the interaction of internal components needs to be carried out. This step also requires a visual representation of the system architecture.

Threat Identification

Once the system architecture is approved, relevant threats compromising the system's structural and procedural integrity must be analyzed. After successfully identifying the threat model to work with, threats can be categorized based on the model's threat identification strategies.

Types of Threat Modeling

OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) methodology is one of the first to be developed in threat modeling. CERT Division of Software Engineering Institute (SEI) from Carnegie Mellon University developed OCTAVE. It is focused on the analysis of the non-technical threats related to organizations. The type of data used for consideration determines the characteristics of the data stored. It is a comprehensive modeling methodology developed to reduce the paperwork in maintaining the assets, but it is not scalable, and scaling can result in rapidly growing unmanageable entities. (Shevchenko, 2018)

PASTA

A PASTA (Process for Attack Simulation and Threat Analysis) is a recently developed threat modeling strategy to provide a set of steps to perform Risk Analysis regardless of the Platform on which the product is hosted. PASTA provides in-depth impact analysis and compliance requirement checks to align business objectives with software requirements. The out from the threat is a score based on threat management and risk enumeration. It is fraud attack-centric to provide the attacker's perspective and related risks. Implementation of PASTA will involve the key stakeholders in the implementation process resulting in comprehensive visibility throughout the implementation process. For companies working on strategic objectives to incorporate impact analysis as a process within the CyberSec responsibilities, PAST threat modeling would be the right choice. This methodology requires an adequately trained team of technologically literate stakeholders in decision-making. (Shevchenko, 2018)

STRIDE

STRIDE comprises the following activities as an acronym: Spoofing, Tampering, Repudiation, Information Message Disclosure, Denial of Service, and Elevation of Privilege. STRIDE aims to provide developers with standards to implement Security Processes while developing the application starting from the design phase. STRIDE guarantees that the characteristics of CIA (Confidentiality, Integrity, and Availability) and AAN (Authorization, Authentication, and Non-Repudiation) are met and are well within the compliance requirements. Due to the involvement of Microsoft, STRIDE hosts extensively documented steps and a vast community of Security SME (Subject Matter Expert) users. (Health Sector Cyber Security Co-ordination Center [HC3] & Department of Health and Human Services [HHS], 2020)

Spoofing Mitigations

As an attack vector, spoofing fundamentally revolves around masquerading as a legitimate entity to deceive systems or individuals, leading to unauthorized access, data theft, or service disruption. The ubiquity of spoofing attacks, spanning domains such as IP, Email, DNS, and ARP, necessitates implementing robust mitigation strategies (Arumugam, 2018). In the context of IP spoofing, implementing network ingress filtering, such as the method described in BCP 38, can effectively block packets originating from illegitimate or spoofed IP addresses (Held, 2020). For egress filtering, employing BCP 84 guidelines helps to prevent the propagation of spoofed packets from one's network. Furthermore, adopting anti-spoofing features in firewalls or routers, including Unicast Reverse Path Forwarding (uRPF), can contribute to a comprehensive defense. Email spoofing, particularly prevalent in phishing attacks, can be mitigated through stringent email authentication protocols, including Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) (Rode, 2022). SPF verifies the sender's IP, and DKIM provides an encrypted signature for message authenticity. At the same time, DMARC unifies the SPF and DKIM authentication mechanisms and specifies a policy on handling messages that fail the authentication. DNS spoofing or cache poisoning, which tampers with the DNS server to redirect traffic, can be thwarted by employing Domain Name System Security Extensions (DNSSEC). DNSSEC offers a layer of security through digital signatures that authenticate the origin of DNS data (Blokdyk, 2018a). Lastly, for mitigating ARP spoofing, a method that manipulates the ARP cache for data interception or network disruption, employing Dynamic ARP Inspection (DAI) in switch configurations or utilizing secure protocols such as SSH or HTTPS for data transmission can provide effective countermeasures (Kovalev, 2020). In essence, given the diverse nature of spoofing attacks, a comprehensive mitigation strategy would necessitate the combined employment of diverse technological and procedural controls, aligning with the specific needs and risks of the environment.

Tampering Mitigations

Tampering is the unlawful change of data, software, or hardware in order to inflict harm, steal information, or circumvent security measures. It poses a serious security risk to enterprises of all sizes and industries, including healthcare facilities. To mitigate tampering, a layered security architecture incorporating powerful technical and procedural safeguards is required (Dumka et al., 2022). Checksums or cryptographic hashes such as SHA-256 can protect data integrity at the data level by detecting unwanted adjustments during the transfer or storage process (Menezes et al., 2019). Furthermore, using secure communication protocols like SSL/TLS and HTTPS helps protect data in transit. Data encryption, during rest and in transit, is additional critical anti-tampering protection that renders data worthless to anybody who has access to it. At the software level, code signing and digital signatures may ensure the validity and integrity of software and firmware, guaranteeing they have not been altered with (Ransome et al., 2022). Regular software updates and patches mitigate vulnerabilities that might be exploited for manipulation. RASP (Runtime program Self-Protection) detects and prevents real-time program modification. Physical tampering can be deterred or detected by tamper-evident and tamper-resistant systems. Tamper-evident designs can show physical interference, but tamper-resistant designs, such as secure hardware modules (SHMs), make tampering exceedingly difficult (Dumka et al., 2022). Tampering is mitigated by administrative and procedural controls such as strict access control regulations, frequent audits, user education, and incident response plans. To maintain data and system integrity, tampering prevention involves a holistic strategy that combines technical protections, procedural controls, and continual monitoring.

Repudiation Mitigations

Repudiation in a security context refers to a situation where an individual or a system denies having acted, usually harmful, without any possibility to prove otherwise. It poses a significant threat to data integrity and can create various legal, financial, and operational problems for organizations (Wang et al., 2018). A comprehensive security strategy is essential to mitigate the risk of repudiation. One primary countermeasure to repudiation is the use of robust authentication mechanisms. Ensuring that users are who they claim to make it more difficult for them to deny actions performed using their credentials (O'Hanley & Tiller, 2020). Non-repudiation services, especially in digital communications, form another significant layer of defense. They ensure that a party involved in communication cannot later deny the authenticity of their electronic messages or documents. The most common form of non-repudiation service is digital signatures, built on public key cryptography, which helps confirm the originator of a document or message (Menezes et al., 2019). Adequate access controls and the principle of least privilege can also help mitigate repudiation by limiting user actions based on their role and responsibilities, thus reducing the likelihood of unauthorized actions (Siegel, 2020). Audit trails and logging are crucial in providing evidence of actions performed in the system. Detailed logging that includes who performed an action, when they performed it, and what the specific action was can help identify irregularities and provide evidence in case of a dispute (Blokdyk, 2018b). User awareness, training, and transparent policies and procedures further enforce accountability and deter potential repudiation attempts (Wang et al., 2018). Mitigating repudiation requires a holistic approach involving strong authentication, non-repudiation services, effective access control, detailed logging, and user education.

Information Disclosure Mitigations

Ensuring the privacy of sensitive data entails a concerted effort towards thwarting access by non-permitted entities, a salient security challenge. An amalgamation of potent security apparatus, legislative tools, and enhanced user cognizance forms the underpinning for safeguarding data during static storage, transmittal, or processing phases (McGregor, 2021). Data encryption is a cornerstone in this technological cordon, morphing intelligible data into an undecipherable cipher text, thus serving as an impenetrable barrier to unauthorized actors lacking the cryptographic key (Golubova & Shumilina, 2022). This safeguard extends equally to data at rest, sequestered in servers or storage devices, and data in transit during its network journey. Moreover, security is further buttressed by employing secure communication frameworks such as HTTPS, and SSL/TLS, posing formidable challenges to any malignant attempts to intercept data in transit (Blokdyk, 2018c). Secure Sockets Layer (SSL) and Transport Layer Security (TLS) proffer a robust bridge between two machines or devices communicating over digital or internetwork channels. Complementing these are effective access control strategies that serve to circumscribe information disclosure. By imposing role-based access control (RBAC), adhering to the principle of least privilege (PoLP), and implementing robust authentication techniques like multi-factor authentication, it can be ensured that access to sensitive information is a privilege afforded only to authorized individuals (Patil, 2018). Systematic security audits and vulnerability assessments constitute another layer of security aimed at identifying and addressing latent system weaknesses, preempting any exploitation, and reducing the risk of information disclosure (Garbis & Chapman, 2021). Rounding off this multifaceted approach is the necessity of user awareness and education. Continual training initiatives and awareness campaigns sensitize users towards the imperative of data confidentiality and the potential risks emanating from unsafe practices (Aloul, 2012). Therefore, the mitigation of information disclosure is predicated on an integrated approach encompassing robust security mechanisms, stringent policies, regulatory safeguards, and an elevated level of user awareness.

Denial of Service Mitigations

Denial of Service (DoS) attacks pose significant threats to service availability by attempting to flood network resources and preventing legitimate users from accessing vital services (Gligor, 2017). A thorough mitigation plan includes technology solutions, strict policy implementation, and user education. Mitigation solutions and services for Distributed Denial of Service (DDoS) are an essential line of defense. These services employ traffic analysis techniques to differentiate between genuine and malicious traffic, banning or restricting the latter (Bhardwaj, 2020). Furthermore, rate restriction can minimize system overload by limiting the number of requests a system will handle from a single source in a given period (Gligor, 2017). Following that, firewalls and intrusion prevention systems (IPS) should be installed to filter out malicious traffic and identify abnormal activity patterns (Alcaraz & Lopez, 2022). Web Application Firewalls (WAF) can also protect against application-level DoS assaults. Proper device security measures should be in place for Internet of Things (IoT) devices frequently targeted for botnet-enabled DoS assaults. These precautions include changing default passwords, upgrading firmware regularly, and deactivating superfluous services (Bhardwaj, 2020). Planning for the incident reaction is also essential. A response strategy for a DoS attack can assist in reducing downtime and damage (Dumka et al., 2022). This includes forming a team to handle such assaults, staying in touch with stakeholders, and collaborating with ISPs and law enforcement organizations. Another critical component is user education since users must understand the hazards and their involvement in avoiding such assaults (Bhardwaj, 2020). Internal DoS assaults can be reduced by providing regular training on optimal practices. Legislative instruments are vital. Laws requiring data protection and network security compliance can prevent potential attackers and hold those responsible for DoS assaults accountable (Gligor, 2017). DoS assaults must be mitigated by an organized approach incorporating sophisticated technology, proactive incident response planning, user awareness, and strict policy enforcement.

Elevation of Privilege Mitigations

In mitigating the considerable security risk posed by privilege escalation, where an unauthorized entity gains unwarranted access to protected resources, a sophisticated defense strategy necessitates multiple layers: technology solutions, rigorous policy enforcement, and continual user education (Garbis & Chapman, 2021). Technology assumes a leading role, underscored by the Principle of Least Privilege (PoLP), which insists on minimal necessary privileges to users or programs, thus constraining the potential havoc wrought by a successful attacker (Viswanathan & J, 2021). User Access Control (UAC), an integral feature of operating systems, actively prompts users before permitting actions requiring higher privileges (Alcaraz & Lopez, 2022). Consequently, proper configuration of these prompts preempts unauthorized privilege elevation. Mandatory Access Control (MAC) and Role-Based Access Control (RBAC) models, which control a user's access based on defined rules and specific roles within an organization, respectively, reinforce these mitigation strategies (Blokdyk, 2018a). Policy enforcement necessitates robust password management, mandating complex, frequently changed passwords, and regular scrutiny of user accounts, facilitating the removal or disabling of redundant ones. Prompt application of security patches, often rectifying vulnerabilities prone to privilege escalation exploitation, is indispensable, as are systematic audits and vulnerability assessments to proactively identify and remedy potential security loopholes (Shevchenko, 2018). Complementing these measures is user education. Awareness programs emphasize the perils of privilege escalation, the significance of security best practices, and, through continual training, considerably diminish the risk of inadvertent privilege escalation (Aloul, 2012). An efficacious strategy for mitigating privilege escalation harmonizes advanced security technologies, robust policy enforcement, and ongoing user training.

Recommended Threat Modeling for a Healthcare Facility

Systems comprising complicated physical and cyber-oriented attributes are primarily distributed and autonomous with multiple access layers and administrations. Such systems require a Threat Model incorporating a spectrum of Threats from various origins. Achieving this within a single TMM is currently not probable. (Shevchenko et al., 2018) The best implementation strategy for such a system with threat remediating requirements would be to implement the PASTA modeling strategy. In addition to PASTA incorporate the STRIDE components to address the gaps in the PASTA modeling.

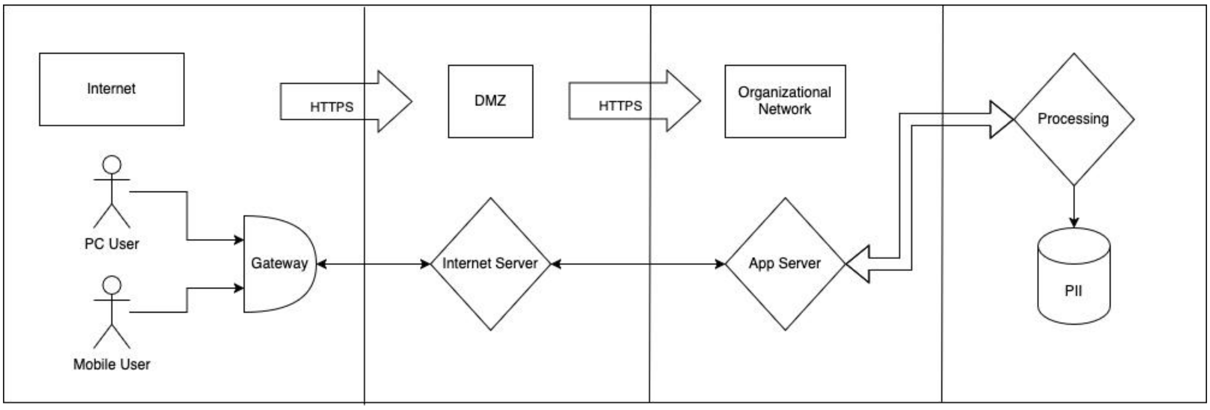

Figure 1 Application Architecture

The PASTA and STRIDE approaches may be integrated to provide a complete threat modeling strategy for healthcare institutions that incorporates a thorough awareness of the threat environment and takes a proactive approach to cyber risks (Willett, 2022). PASTA is a seven-step risk-centric approach to threat modeling that aims to integrate business objectives with technological needs while detecting and analyzing possible risks. PASTA aids in system comprehension, threat detection, and analysis, culminating in countermeasure identification and deployment (Le & Hoang, 2017). This technique, with its structured, risk-based approach, provides a strategic assessment of the threat environment particular to healthcare institutions. STRIDE assists in the identification of threats depending on the sort of illegal behavior that could take place in a system. While PASTA is primarily concerned with the process, STRIDE is concerned with finding and categorizing hazards (Martin, 2022). Incorporating STRIDE into PASTA modeling can improve PASTA's threat detection phase, resulting in a more complete and detailed threat picture. STRIDE can explain particular threat kinds, giving depth to PASTA's wide identification and therefore reducing inadequacies in threat enumeration (Mead & Shoemaker, 2021). Furthermore, STRIDE can help PASTA's threat analysis phase by assessing threats based on their possible impact on the system. Understanding how each threat type (as defined by the STRIDE classification) might jeopardize the security objectives of confidentiality, integrity, and availability allows healthcare institutions to develop an effective, focused mitigation approach (Martin, 2022). Introducing STRIDE components into PASTA modeling will improve healthcare institutions' capacity to predict, identify, assess, and reduce dangers. This comprehensive approach will strengthen healthcare systems' resilience, creating a strong defense against the many cyber dangers of the modern digital era.

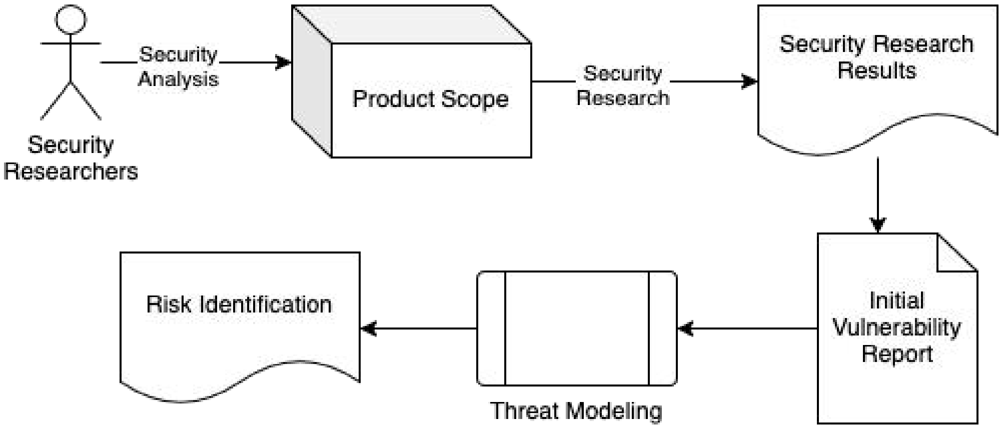

Figure 2 Threat modeling and Risk Identification

Reason for Recommendation

Adaptability

Integral to proactive security management, the Process for Attack Simulation and Threat Analysis (PASTA) strategy exemplifies unique adaptability through its unification of business and technical requirements, a versatile threat modeling approach suitable for the ever-evolving cyber threat landscape (De, 2020). This adaptability, at the heart of PASTA's seven-step iterative cycle, promotes continual improvement, with each phase definition, identification, exploration, attack enumeration, vulnerability analysis, risk analysis, and countermeasure proposal adjustable to current security objectives, threat intelligence, and organizational transitions (Dumka et al., 2022). The result: a perpetually updated threat model accurately mirroring the system's state, vulnerabilities, and potential threats. PASTA's adaptability, underscored by its contemplation of multiple attacker profiles and potential attack vectors, permits the refinement of defenses according to realistic threat scenarios (Martin, 2022). Such adaptability extends to its incorporation with broader security practices, including the Security Development Lifecycle (SDL) and DevOps methodologies (Ransome et al., 2022; Umeugo, 2023). This amalgamation fosters the weaving of threat modeling into comprehensive security and software development processes, advocating for Security by design, a paradigm resonating with contemporary best practices (De, 2020). The adaptive PASTA strategy, encapsulating iterative processes, realistic threat scenarios, and integration with broader security methodologies, aligns effortlessly with an organization's fluid security requisites.

Integration

PASTA's inherently adaptable methodology engenders up-to-date, dynamic threat models. At the same time, STRIDE hones this strategic approach to a fine point, zeroing in on specific threats, including spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege (Martin, 2022). Thus, through the combination of these methods, software systems are armored against the mutable face of cyber threats, and a potent blend of thoroughness, inclusivity, and adaptability characterizes the resultant strategy.

Risk and Effect

PASTA incorporates the Risk and Effect analysis to remediate the threat explosion from the STRIDE modeling. Therefore, a high-level implementation of the PASTA strategy along with STRIDE for threat identification and analysis could provide the best possible outcome in securing the product.

Phase-by-Phase Implementation

Define Business Objectives

Align security goals with the organization’s mission and regulatory requirements. Identify the most critical healthcare processes (e.g., electronic health record [EHR] management, patient admission, claims processing). Map regulatory requirements such as HIPAA or GDPR to ensure that confidentiality, integrity, and availability controls are built into the design from the start. During this phase, the STRIDE categories should be presented to key stakeholders so they understand the types of threats that may arise. (Naik et al., 2024) Any prior threat intelligence or incident history within the healthcare sector (e.g., past ransomware attacks) should be discussed to set the scope.

Define the Technical Scope

Specify the systems, applications, and data flows that will be analyzed. Document the technical architecture of EHR systems, telehealth platforms, networked medical devices, and supporting infrastructure. (Abuabed et al., 2023) Pay particular attention to data flows between clinical devices, on-premises servers, and cloud services. To ensure comprehensive coverage, start mapping each system or subsystem to relevant STRIDE threat categories. For instance, a telehealth application may be prone to Spoofing or Information Disclosure, while a PACS (Picture Archiving and Communication System) often faces threats related to Denial of Service.

Application Decomposition

Break down the application into logical components (servers, databases, user interfaces, external integrations). Decompose healthcare workflows, including patient registration, medication administration, and lab reporting. Identify where Protected Health Information (PHI) is stored or transmitted and detail data-entry points where vulnerabilities can emerge. (Abuabed et al., 2023) Create data-flow diagrams and map each flow against STRIDE threat types (e.g., label flows that might be vulnerable to Spoofing attacks or store sensitive data that could be subject to Information Disclosure).

Threat Analysis

Enumerate potential threats based on discovered vulnerabilities and threat vectors. Cross-reference known threats (e.g., ransomware, phishing, insider threats, unauthorized access to medical devices) with the decomposition from Phase 3. Leverage STRIDE as a structured checklist to identify threats systematically. (Abuabed et al., 2023) Assess how each STRIDE category may manifest in the healthcare environment.

Vulnerability Detection

Identify and validate existing vulnerabilities in the system. Conduct vulnerability scanning and penetration testing on critical healthcare applications (e.g., EHR modules handling patient prescriptions). Integrate known vulnerabilities from regulatory advisories or medical device manufacturer bulletins. (Naik et al., 2024) Map discovered vulnerabilities to specific threat categories. For instance, a missing input validation in a patient portal may be mapped to both Tampering and Information Disclosure, enabling more precise remediation planning.

Threat Enumeration and Scoring

Score threats based on severity, likelihood, and potential impact on patient safety and organizational reputation. Prioritize threats that could disrupt patient care or expose large volumes of PHI. Consider compliance penalties, patient safety implications, and reputational risks as key impact factors. (Abuabed et al., 2023) Group and rank threats by STRIDE category to maintain a clear taxonomy, highlighting high-risk items (e.g., Denial of Service on emergency services) that need immediate attention.

Risk and Impact Analysis

Develop strategic mitigation and remediation plans based on calculated risk levels. Recommend safeguards and incident response protocols specific to each high-risk threat. Examples include encrypting stored PHI, implementing multifactor authentication for staff, and isolating critical medical devices from general hospital networks. (Naik et al., 2024) Document which STRIDE category each mitigation addresses so that healthcare leaders can track improvements in threat coverage.

Conclusion

Implementing successful threat modeling strategies necessitates an organization's prowess in risk identification, threat quantification and consolidation, and delivering consistent threat identifications (Shevchenko et al., 2018). These critical outcomes collectively enhance the organization's understanding of the threat landscape, thereby fostering a climate of cybersecurity resilience. The challenge lies, however, in the judicious selection of the optimal threat modeling strategy during nascent stages of development, dictated solely by the product's objectives.

Foremost in threat modeling considerations is the model's scalability at a business level and its capacity to satiate reporting requirements. In essence, an effective threat model should offer potent, actionable insights derived from identified threats and areas warranting enhancement (Shevchenko, 2018). This objective transcends mere technical facets, implicating broader organizational perspectives and aligning with overarching business goals. A scalable model enables organizations to account for evolving threats, business expansion, and technological advancements, ensuring the maintenance of a dynamic and updated security posture.

Simultaneously, the model should cater to the organization's reporting needs, delivering lucid, insightful analysis of the threat landscape. These reports, in turn, can inform strategic decision-making processes, driving the organization toward a more proactive and comprehensive cybersecurity stance. (Abuabed et al., 2023) Thus, the model's effectiveness hinges on its capability to translate identified threats and potential improvements into meaningful, strategic insights.

Conflict of Interest

The authors declare that they have no conflicts of interest to this work.

References

Abernathy, R., & Hayes, D. R. (2022). *Cissp cert guide* (4th ed.). Pearson IT Certification.

Alcaraz, C., & Lopez, J. (2022). Digital twin: A comprehensive survey of security threats. *IEEE Communications Surveys & Tutorials, 24*(3), 1475–1503. https://doi.org/10.1109/comst.2022.3171465

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology, 3*(3). https://doi.org/10.4304/jait.3.3.176-183

Alshehri, S., Mishra, S., & Raj, R. (2013). Insider threat mitigation and access control in healthcare systems. *RIT Scholar Works,* (1401). https://doi.org/http://scholarworks.rit.edu/article/1401

Amini, A., Jamil, N., Ahmad, A., & Z`aba, M. (2015). Threat modeling approaches for securing cloud computin. *Journal of Applied Sciences, 15*(7), 953–967. https://doi.org/10.3923/jas.2015.953.967

Arumugam, D. N. (2018). A survey of network-based detection and defense mechanisms countering the ip spoofing problems. *International Journal of Trend in Scientific Research and Development, Volume*-2(Issue-5), 704–710. https://doi.org/10.31142/ijtsrd15921

Bhardwaj, A. (2020). *Ddos attack mitigation architecture*. LAP LAMBERT Academic Publishing.

Blokdyk, G. (2018a). *Application security requirements and threat management standard requirements* (28th ed.). Emereo.

Blokdyk, G. (2018b). *Computer security incident management: A practical guide*. CreateSpace Independent Publishing Platform.

Blokdyk, G. (2018c). *Tls transport layer security standard requirements* (18th ed.). Emereo.

Butcher, C., & Hussain, W. (2022). Digital healthcare: The future. *Future Healthcare Journal, 9*(2), 113–117. https://doi.org/10.7861/fhj.2022-0046

De, S. (2020). Security threat analysis and prevention towards attack strategies. In (Ed.), *Cyber defense mechanisms* (pp. 1–22). CRC Press. https://doi.org/10.1201/9780367816438-1

Dumka, A., Ashok, A., Verma, P., Bhardwaj, A., & Kaur, N. (2022). Security in wireless sensor networks – background. In (Ed.), *Security issues for wireless sensor networks* (pp. 15–39). CRC Press. https://doi.org/10.1201/9781003257608-2

Elmasry, W. (2019). *Intrusion detection using deep learning* (1st ed.). LAP LAMBERT Academic Publishing.

European Union Agency for Cybersecurity. (2016). *Smart hospitals: Security and resilience for smart health service and infrastructures*. https://doi.org/https://data.europa.eu/doi/10.2824/28801

Fichman, R. G., Dos Santos, B. L., & Zheng, Z. (2014). Digital innovation as a fundamental and powerful concept in the information systems curriculum. *MIS Quarterly, 38*(2), 329–343. https://doi.org/10.25300/misq/2014/38.2.01

Fu, J.-S., Liu, Y., Chao, H.-C., Bhargava, B. K., & Zhang, Z.-J. (2018). Secure data storage and searching for industrial iot by integrating fog computing and cloud computing. *IEEE Transactions on Industrial Informatics, 14*(10), 4519–4528. https://doi.org/10.1109/tii.2018.2793350

Furukawa, M. F., Raghu, T. S., & Shao, B. M. (2010). Electronic medical records, nurse staffing, and nurse-sensitive patient outcomes: Evidence from california hospitals, 1998-2007. *Health Services Research, 45*(4), 941–962. https://doi.org/10.1111/j.1475-6773.2010.01110.x

Garbis, J., & Chapman, J. W. (2021). Intrusion detection and prevention systems. In (Ed.), *Zero trust security* (pp. 117–126). Apress. https://doi.org/10.1007/978-1-4842-6702-8_8

Gariépy-Saper, K., & Decarie, N. (2021). Privacy of electronic health records: A review of the literature. *Journal of the Canadian Health Libraries Association / Journal de l'Association des bibliothèques de la santé du Canada, 42*(1). https://doi.org/10.29173/jchla29496

Georgakopoulos, D., & Jayaraman, P. (2016). Internet of things: From internet scale sensing to smart services. *Computing, 98*(10), 1041–1058. https://doi.org/10.1007/s00607-016-0510-0

Gligor, V. D. (2017). Defending against evolving ddos attacks: A case study using link flooding incidents (transcript of discussion). In (Ed.), *Security protocols xxiv* (pp. 58–66). Springer International Publishing. https://doi.org/10.1007/978-3-319-62033-6_8

Golubova, A., & Shumilina, V. (2022). Information security and data protection in modern society. *Science & World, 0*(2), 6–10. https://doi.org/10.26526/2307-9401-2022-2-6-10

Goniewicz, M. (Ed.). (2022). *Disasters preparedness and emergency response: Prevention, surveillance and mitigation planning* (M. Goniewicz, Ed.). MDPI. https://doi.org/10.3390/books978-3-0365-6056-4

Health Sector Cyber Security Co-ordination Center & Department of Health and Human Services. (2020). *Threat Modeling for Mobile Health Systems* (Leadership for IT Security and Privacy Across HHS Report : 202004301030) [Report]. https://www.hhs.gov/sites/default/files/threat-modeling-mobile-health-systems.pdf

Held, G. (2020). Protecting a network from spoofing and denial of service attacks. In *Network design* (pp. 659–666). Auerbach Publications. https://doi.org/10.1201/9781420093759-58

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems, 43*(2), 618–644. https://doi.org/10.1016/j.dss.2005.05.019

Jumani, A., Siddique, W., & Laghari, A. (2023). Cloud and machine learning based solutions for healthcare and prevention. In (Ed.), *Image based computing for food and health analytics: Requirements, challenges, solutions and practices* (pp. 163–192). Springer International Publishing. https://doi.org/10.1007/978-3-031-22959-6_10

Jusob, F., George, C., & Mapp, G. (2021). A new privacy framework for the management of chronic diseases via mhealth in a post-covid-19 world. *Journal of Public Health, 30*(1), 37–47. https://doi.org/10.1007/s10389-021-01608-9

Kovalev, M. (2020). Tracing network packets in the linux kernel using ebpf. *Proceedings of the Institute for System Programming of the RAS, 32*(3), 71–77. https://doi.org/10.15514/ispras-2020-32(3)-6

Le, N. T., & Hoang, D. B. (2017). Capability maturity model and metrics framework for cyber cloud security. *Scalable Computing: Practice and Experience, 18*(4). https://doi.org/10.12694/scpe.v18i4.1329

Lee, S. M., & Lee, D. (2020). Healthcare wearable devices: An analysis of key factors for continuous use intention. *Service Business, 14*(4), 503–531. https://doi.org/10.1007/s11628-020-00428-3

Liu, C., Tan, C.-K., Fang, Y.-S., & Lok, T.-S. (2012). The security risk assessment methodology. *Procedia Engineering, 43*, 600–609. https://doi.org/10.1016/j.proeng.2012.08.106

Luttmer, E. P., & Samwick, A. A. (2018). The welfare cost of perceived policy uncertainty: Evidence from social security. *American Economic Review, 108*(2), 275–307. https://doi.org/10.1257/aer.20151703

Malamas, V., Chantzis, F., Dasaklis, T. K., Stergiopoulos, G., Kotzanikolaou, P., & Douligeris, C. (2021). Risk assessment methodologies for the internet of medical things: A survey and comparative appraisal. *IEEE Access, 9*, 40049–40075. https://doi.org/10.1109/access.2021.3064682

Martin, T. (2022). Software attacks and threat modeling. In (Ed.), *Designing secure iot devices with the arm platform security architecture and cortex-m33* (pp. 223–257). Elsevier. https://doi.org/10.1016/b978-0-12-821469-5.00004-1

McGregor, S. E. (2021). *Information security essentials* (3rd ed.). Columbia University Press.

Mead, N. R., & Stehney, T. (2005). Security quality requirements engineering (square) methodology. *ACM SIGSOFT Software Engineering Notes, 30*(4), 1–7. https://doi.org/10.1145/1082983.1083214

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2019). Overview of cryptography. In (Ed.), *Handbook of applied cryptography* (pp. 1–48). CRC Press. https://doi.org/10.1201/9780429466335-1

Ngai, E., Moon, K. K., Riggins, F. J., & Yi, C. Y. (2008). Rfid research: An academic literature review (1995–2005) and future research directions. *International Journal of Production Economics, 112*(2), 510–520. https://doi.org/10.1016/j.ijpe.2007.05.004

Office for Civil Rights. (2009, November 19). *Summary of the hipaa security rule* (Last Reviewed October 19, 2022). HHS.gov. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Patil, S. (2018). *Data protection through purpose & role based access control in rdbms* (1st ed.). LAP LAMBERT Academic Publishing.

Ransome, J. F., Anmol, & Merkow, M. S. (2022). The security development lifecycle. In (Ed.), *Practical core software security* (pp. 15–46). Auerbach Publications. https://doi.org/10.1201/9781003319078-2

Risk measures with applications in finance and economics. (2019). Mdpi AG.

Rode, O. O. (2022). Email spam protection technology based on dmarc. *Modern Information Security, 3*(51). https://doi.org/10.31673/2409-7292.2022.033238

Schmeelk, S. (2019). Where is the Risk? Analysis of Government Reported Patient Medical Data Breaches. *IEEE/WIC/ACM International Conference on Web Intelligence*. https://doi.org/10.1145/3358695.3361754

Seh, A., Zarour, M., Alenezi, M., Sarkar, A., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare data breaches: Insights and implications. *Healthcare, 8*(2), 133. https://doi.org/10.3390/healthcare8020133

Shevchenko, N. (2018). *Threat Modeling: 12 Available Methods*. Carnegie Mellon University's Software Engineering Institute. https://doi.org/http://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

Shevchenko, N., Frye, B. R., & Woody, C. (2018). Threat modeling: evaluation and recommendations. *Software Engineering Institute*, REV 03. https://doi.org/https://apps.dtic.mil/sti/pdfs/AD1083907.pdf

Siegel, C. A. (2020). Internet security architecture. In (Ed.), *new directions in internet management* (pp. 565–576). Auerbach Publications. https://doi.org/10.1201/9780203997543-58

Sokolnikov, A. U. (2017). *Graphene for defense and security* (1st ed.). Taylor & Francis.

Topol, E. J. (2019). High-performance medicine: The convergence of human and artificial intelligence. *Nature Medicine, 25*(1), 44–56. https://doi.org/10.1038/s41591-018-0300-7

Umeugo, W. (2023). Secure software development lifecycle: A case for adoption in software smes. *International Journal of Advanced Research in Computer Science, 14*(01), 5–12. https://doi.org/10.26483/ijarcs.v14i1.6949

Viswanathan, G., & J, P. (2021). A hybrid threat model for system-centric and attack-centric for effective security design in sdlc. *Web Intelligence, 19*(1-2), 1–11. https://doi.org/10.3233/web-210452

Wang, Y., Kung, L., & Byrd, T. (2018). Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. *Technological Forecasting and Social Change*, 126, 3–13. https://doi.org/10.1016/j.techfore.2015.12.019

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health, 4.* https://doi.org/10.3389/fdgth.2022.862221

What is digital forensics, and what should you know about it? (2020). In O'Hanley, R., & Tiller, J. S. (Eds.), *Digital forensics explained* (pp. 24–35). Auerbach Publications. https://doi.org/10.1201/b13689-6

Willett, K. D. (2022). Systems thinking and security. In (Ed.), *Handbook of security science* (pp. 553–572). Springer International Publishing. https://doi.org/10.1007/978-3-319-91875-4_94

Wu, I.-L., Li, J.-Y., & Fu, C.-Y. (2011). The adoption of mobile healthcare by hospital's professionals: An integrative perspective. *Decision Support Systems, 51*(3), 587–596. https://doi.org/10.1016/j.dss.2011.03.003

Zhang, X., Liu, C., Nepal, S., Pandey, S., & Chen, J. (2013). A privacy leakage upper bound constraint-based approach for cost-effective privacy preserving of intermediate data sets in cloud. *IEEE Transactions on Parallel and Distributed Systems, 24*(6), 1192–1202. https://doi.org/10.1109/tpds.2012.238

Zhao, Y., Cui, M., Zheng, L., Zhang, R., Meng, L., Gao, D., & Zhang, Y. (2019). Research on electronic medical record access control based on blockchain. *International Journal of Distributed Sensor Networks, 15*(11), 155014771988933. https://doi.org/10.1177/1550147719889330

Naik, N., Jenkins, P., Grace, P., Naik, D., Prajapat, S., Song, J. (2024). A Comparative Analysis of Threat Modelling Methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. The International Conference on Computing, Communication, Cybersecurity and AI, July 3–4, 2024, London, UK. C3AI 2024. Lecture Notes in Networks and Systems, vol 884. Springer, Cham. https://doi.org/10.1007/978-3-031-74443-3_16.

Abuabed, Zaina., Alsadeh, Ahmad., Taweel, Adel. STRIDE threat model-based framework for assessing the vulnerabilities of modern vehicles (2023). *Computers & Security, Volume 133.* https://doi.org/10.1016/j.cose.2023.103391

How to Cite: Ramakrishnan, R., Panneerselvan, B., Rakkiappan, P & Rudrashetty, M. (2025). Threat Modeling - Recommendations for a Health Care Facility. *Journal of Global Humanities and Social Sciences*, *6*(3), 86-100. https://doi.org/ 10.61360/BoniGHSS252017920303