Journal of Theoretical and Applied Information Technology
15th April 2024. Vol.102. No 7
© Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

OVERVIEW OF CYBERSECURITY RISK ASSESSMENT FOR MEDICAL INFORMATION SYSTEMS

TAYSEER ALKHDOUR[1], MOHAMMED ALMAIAH[2, 3], KHALIL IBRAHIM ALMUWAIL[1], MOHMOOD A. AL-SHAREEDA[4], THEYAZAN ALDAHYANI[5] AND RANA ALRAWASHDEH[6]

[1] College of Computer Science and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[2] King Abdullah the II IT School, the University of Jordan, Amman 11942, Jordan
[3] Applied Science Research Center, Applied Science Private University, Amman 11931, Jordan
[4] Department of Communication engineering, Iraq University College, Basra, Iraq
[5] Applied College in Abqaiq, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[6]King Fahd of Petroleum and Mineral, Faculty of computer science and information system, Dhahran 31261, Saudi Arabia

Corresponding author: talkhdour@kfu.edu.sa and m.almaiah@ju.edu.jo

ABSTRACT

In recent years, there has been a significant increase in demand for hospital information systems in healthcare institutions. Data security, on the other hand, is a significant concern with regard to using health information systems. The purpose of this research is to examine the security risk assessment of medical information systems. This study involves a systematic evaluation of the literature to provide a complete overview of previous articles and research on Security Risk Assessment in Medical Information Systems. For this research, a qualitative and descriptive research design was applied. Scientific literature, as well as recent articles from popular publications, will be evaluated and analyzed in depth in accordance with the study design. A review of the literature enables a thorough comprehension and knowledge of this subject, Security Risk Assessment in Medical Information Systems. It provides the background for the research and provides an overview of the study's relationship to a large field of study. The main objective of this research has to analyze and discuss the findings of the literature review, and to evaluate the risks and challenges. Moreover, each study was examined in terms of methodology, threats addressed, and suggested mitigations. Additionally, the study discussed the systematic review's gaps and major neglected concerns, as well as future directions in risk assessment in medical information systems.

Keyword: *Medical Information Systems; Cybersecurity; Risk Assessment; Information Security.*

1. INTRODUCTION

Several studies have been conducted on the possible risks of cyberattacks, particularly in healthcare organizations. There are, however, a number of unknown risks that might threaten the privacy of healthcare resources and information, in healthcare centers. A risk assessment is a procedure in which people identify dangers and decide the most effective means of avoiding or controlling those threats. Healthcare information security mainly depends on risk assessment. Regardless of their size, every medical center must assess the risks and provide an up-to-date detailed record of the performance. A wide range of internal and external security risks, such as the exploitation and risks of important information, affect the security of organizations today [1]. Natural catastrophes and human errors may also pose a danger to cyber security, which might result in serious outcomes [2]

Protecting personal information security, maintaining information integrity, and securing system reliability all conform to the requirements of health data security. Hospitals and other healthcare organizations may face legal challenges or economic damages if they fail to address any of these issues [3]. Improved information privacy, on the other hand, might lead to improved access to healthcare records by patients and healthcare professionals equally [4]. Illegal technology and software used for communication and crimes are the most prevalent dangers to data security. Rejected workers may pose a new danger to information security, thus the level of permission provided to these individuals should be limited. Hacker, privacy breaches, and Computer viruses may also compromise the security of the information [5]. Therefore, it is important to recognize the cybersecurity risks in healthcare in order to be allowed to deal with the possible consequences in the future. A risk management plan is essential in order to avoid problems caused by a range of security risks [6].

Evaluating security risks, estimating the likelihood and impact of possible threats, and finally, evaluating the threats to identify the proper level of practice and policies required for successful management are some of the ways for evaluating cybersecurity risks [7]. For healthcare organizations, risk assessment is necessary to correctly manage resources, plan human resource management, comply with their global regulatory requirements, and protect their property and patients' data [8]. The goal of this study is to assess the information security risks in medical information systems.

1.2 Motivation

Comparable to other sectors, hospitals are also susceptible to threats. At the same time, healthcare organizations are urged to adopt electronic health records and to share them with one another. They are particularly susceptible to data threats because of the significance of their healthcare information [9]. Hence, healthcare organizations have a challenge in securing healthcare information. Therefore, it is crucial to explore this subject and look for solutions to lower these threats. It is important to examine the types of threats, the strategies employed, and how to defend against these risks. Thus, this study will focus on the most important issues.

The main problem affecting hospitals today is the exploitation and threats of patient information, both of which threaten the security of the organizations [10]. Personal data security, data management, and system reliability are primary needs of health data security. Hospitals and other healthcare organizations may suffer social or legal consequences if they ignore these risks. Because of the significance of their medical records, they are particularly vulnerable to security threats. Hence, healthcare organizations have a problem with the protection of healthcare data. Thus, this study must present the risk assessment of information security in medical information systems and how people with less experience may protect themselves from these cyberattacks

The scope of this research is mainly on the assessment of information security threats of medical information systems and how these risks might be mitigated by people. The findings of the study can be applied to healthcare organizations to improve the efficiency of the IT departments and the security of patient data. The research will encourage people to protect themselves by focusing on the risks associated with information security. It describes the measures hospitals have taken to improve their strategies to provide better data security and patient identification. The main objectives of the study including:

1. To review the Information Security Risk Assessment for medical information systems.
2. To analyze the information security threats, solution and assessment for medical information systems.

2. LITERATURE REVIEW

This sections presents the literature of Security Risk Assessment in Medical Information Systems. An IoT risk assessment framework was suggested by [11] as a step-by-step procedure for IoT risk assessment in a healthcare system. DEMATEL IoT Threat Assessment Technique was used to construct the suggested risk control framework for IoT. On the basis of a particular hospital's recent use of IoT technology, that research was conducted. In a survey with selected participants from the health center, it was found that specific case study did not have a developed IoT risk management framework because of the ad hoc IoT deployment method. Healthcare information is not adequately protected in the research study, which also has various alternate work processes. Three IoT specialists and two IT health providers assessed the suggested model using the System Usability Score (SUS) and gave it a Good Usability Score, indicating that it may be used to control healthcare IoT risks. Each stage of the risk assessment must be protected by system security organizations to guarantee that solutions are being followed. Healthcare's important services might hold down development and improvement. Risk management teams must work effectively to keep the service operating smoothly. Assessment may assist administrators to understand what adjustments need to be done to maintain the essential risk management within the organization, as well as identify technical controls that are lacking [12].

Another research by [13] examined a strategy for a standardized risk assessment library and an example use case that relates the findings of a risk web application risk assessment to the developed standardized library. An open-source risk assessment systematic framework was developed as a result of this study. An open-source risky web application was used to show the advantages of using a standard risk management framework. According to the results, this use case demonstrates how well the framework may be used to standardize language for the risk management process and thereby improve the overall system. Strategic planning and assessing risk across organizations is inefficient if each member in the organization adopts their own personal language to explain risk components. This kind of risk assessment need has yet to be addressed by a standardized library. This study describes a standardized framework and provides an example of how it may be put to use [14].

At Moi Teaching and Referral Hospital, the research by [15] introduced a new way of protecting the security of the Hospital Information System against the risk of the patient data breach. For a secure electronic health record, this framework offers an organized system for implementing data security and the essential strategies, methods, policies, and technology to assure privacy and data security. The findings also show that most operational safety precautions, such as regulations and guidelines, are in place and help more to data security. Most of the medical records workers seem to believe that the privacy policy and restrictions in place are effective. In contrast to organizational information security, the most of staff members disagreed on technological and organizational security requirements.

Risk management for a patient's information technology (IT) security system was investigated by [16]. The model was implemented by examining existing information security risk analysis standards and guidelines. Important strategies like Risk Evaluation and Security Risk Evaluation were included in the risk evaluation. The system was able to investigate and assess the security risk associated with the hospital's information management system based on the findings of the research at selected hospitals. This system was capable of predicting many exploitation scenarios in order to identify security breaches and develop a standard analysis. An evaluation of models found that they were capable of changing the levels of data security in an accurate representation of healthcare facilities. Additionally, the prototype system was able to analyze a risk management plan with solutions for improving security [16].

Flexible risk management frameworks for healthcare systems were developed by [17] in the area of management reliability. In addition, a strategy for creating a successful continuity plan was provided. Risk analysis of various kinds of security systems in various organizations may be achieved by obtaining the necessary information using the presented strategy. Implementing a statistical method for allocating resources in the face of potential threats might be regarded as a future research. This research did not consider probable correlations between impact variables in order to keep the risk assessment process from becoming more difficult. Furthermore, these interactions may be explored using an effective approach such as DEMATEL or fuzzy cognitive maps [17].

For the Internet of medical things (IoMT) [18] proposed a taxonomy of security and privacy issues (S&P). The technique for quantifying IoMT risk and demonstrating risk assessment in two IoMT devices were also discussed. By allowing IoMT participants to evaluate and assess possible S&P risks, this effort intends to raise S&P knowledge among IoMT participants. S&P of IoMT is significantly more challenging because of its vulnerability and importance in hospitals, which makes it even more challenging. Patients' security and even health might be concerned if IoMT does not have adequate S&P in order. Efficient security strategies may be designed with the taxonomy's aid in comprehending the IoMT S&P concerns. There may be novel or unknown risks and attributes that need to be addressed in the future because of the fast advancement of technology and hacking abilities. Based on the taxonomy, researchers came up with a risk assessment method. The suggested risk assessment intends to aid users in understanding and measuring security in IoMT so that they may make better decisions. Researchers were planning to create more measures to help in the quantification of IoMT S&P. Researchers anticipate that their study will aid in the adoption and development of safe IoMT, so that patients and healthcare professionals may benefit greatly while posing a low risk [19].

[20] Conducted an evaluation of the Health Information System of hospitals affiliated with a university of medical sciences in western Iran. All healthcare departments have been connected to the Health Information System (HIS) by a Local Access Network (LAN). It is critical to design and operate this technology while keeping in mind the demands of users, existing procedures, and organizational structures. The effectiveness of these systems depends on the ability to adjust HIS to the specific demands of system customers. Information from both medical and non-clinical sectors of healthcare institutions was collected using a five-point Likert scale survey. Descriptive statistical analysis was employed to analyze the data in SPSS program. Even though all health care facilities acquired their software from a single software firm, the level of user experience with different components of systems was practically the same, according to the findings. It was recommended that web-based HIS capabilities, international database information, and software module adaptability be implemented as the most significant system improvement [21].

In a research, [22] proposed an assessment tool for security threats. A total of 125 publications published between 1995 and May 2014 were used to develop this analysis. Depending on the size of the company, risk assessment approaches might be difficult to choose. Since the previous taxonomy does not take into account or apply significant criteria in risk assessment created by new technological developments or the level of awareness of a hacker, numerous risk-based solutions have been proposed. An information security policy included the most important aspects of risk management, according to researchers. Organizations may use the novel risk management taxonomy to perceive risk assessment by assessing different new ideas, as well as choosing an appropriate method for conducting a risk assessment. Furthermore, this taxonomy will offer up potential opportunities for study in the rapidly expanding area of risk evaluation. This study's taxonomy is a step forward in terms of establishing high-quality information security risk assessment [22].

[23] analyzed the private financing initiative (PFI) in the hospital industry's developments and risk evaluation. The research evaluated secondary information and conducted interviews with different individuals in large healthcare PFI research s in order to have better understanding of recent advancements in healthcare PFI and risk assessment in healthcare programs. According to the findings, the quantity, capital growth, and scale of healthcare research s using PFI are all on the rise. Risks control strategies of various degrees of severity were used in the hospital PFI research. It appears that the primary risk assessment method used was experienced, whereas prevention was initially examined before assessing and assigning any remaining risks. Additionally, the usage of "Risk Warning" tools, such as risk matrix and assessments, helped to identify hazards. There seems to be a strong emphasis on security and contracting as risk management tools among all players. Risk management strategies employed in PFI research s, although general, have not yet been shown to be applicable for this kind of research. It is crucial that more analysis be carried out to determine the present degree of risk management strategies and the level to which these strategies are adequate for complicated hospital PFI research s [24].

The adoption of electronic healthcare systems in health facilities has risen significantly in many countries. However, the most significant problem with electronic healthcare systems utilization is the security of data. Research conducted by [25] evaluated the risk management of electronic healthcare systems in hospital services with respect to information privacy. A qualitative and cross-sectional approach is used in this experimental analysis. In Iran, 551 hospitals were surveyed for this study. The Health ministry in Iran issued an intense survey to all healthcare institutions in Iran to evaluate the security risk planning and implementation at the concerned hospitals, based on a study of literature, specialists' views, and investigations at medical centers. According to the Iran Healthcare Assessment Criteria, 69% of the hospitals in the study implement an information security management system. Identifying and evaluating risks have all been unorganized processes at some medical facilities. The investigated hospitals lack a systematic strategy to risk assessment [25].

In a study, [26] presented measures to protect information acquired by the industry, as well as to enable faster and more secure transaction records. The secondary data was obtained from relevant sources. Primary data were obtained using an internet search engine. Information was used to conduct the quantitative and qualitative analysis that was completed. For this study, the collected data were analysed quantitatively. For this study, the collected data were analysed quantitatively. Cybersecurity instances have surged despite the health sector's adoption of electronic healthcare and security. Cybersecurity cases were studied in an effort to identify characteristics that may impact the number of breaches. In light of the present crisis, it was concluded that the healthcare industry had prospects in the electronic healthcare sector. Cybersecurity has been a concern since cyberattacks have stolen personal data and taken severe efforts to minimize the same [26].

Data protection attitude and risk assessment across healthcare professionals were evaluated by [27]. The information technology security climatic change indicator, designed and verified on two proposed datasets, was based on the organizational context literature and has been intended to influence employee behaviour. As a part of the investigation, 4 healthcare workers (clinical nurse assistants, orthodontists, pharmacists, and medical assistants) were interviewed. The Cybersecurity Context Measure, data security intention, and data security behaviors were assessed using Likert-type questions. The Data Security Context Measure was shown to be associated with higher levels of security-related motivation and behaviour among employees. Health care workers reported a more pleasant working environment and more positive attitudes about their colleagues than did pharmacists. The researchers came to the conclusion that security breaches would probably remain in the near future. Considering insecurities about cybercriminals, most of the threat is caused by irresponsible and/or criminal employee actions. Change in behavior may be achieved via an organizational climate strategy. Research has shown that a company's data security policy affects employee behavior, therefore it may be useful in influencing attitudes about data protection and privacy [28].

Using fuzzy analytic hierarchy processes, [29] evaluated web-based healthcare information framework potential risks. Each and every component of useable security was examined in detail by the researcher. When designing a health online system, this will assist clinicians in improving both usability and cybersecurity. The hospital digital system's efficiency and security were examined in this study. Furthermore, the opinions of 101 web development professionals and academics on six security risk indicators were considered. Fuzzy AHP was used to calculate the weight of each security element based on this judgment. According to the findings of the research, user experience has to be the most important factor to consider when assessing security risks. Developers of healthcare web applications must put an emphasis on user experience if they want to achieve optimum system operations [29].

In a study, [30] evaluated the university hospital systems' organizational, technological, and digital security to determine their current state of information systems. Information systems professionals (n=36) from healthcare institutions linked with the top-ranked healthcare centers (University A and University B) took part in this research study. A questionnaire was used to collect the information needed to complete the study. To ensure the questionnaire's accuracy, professionals assessed its internal consistency and assessed its consistency using Cronbach's coefficient alpha (α=0.75). Organizational protections were found to be set at a medium level, according to the findings. Information technology administrators assessed the physical and technological protections at a very high level. The findings show that administrative protections were given a medium-security assessment out of three possible options. Implementing security rules, putting in place user access frameworks, and training users have all been suggested to increase cybersecurity [30].

In a research, [31] conducted field research to investigate the risk variables associated with the implementation of operating systems in a medical IT system and developed a risk management system and evaluations for identifying potential risks. In this study, the primary goal is to develop an information security risk management system for the healthcare sector. In this study, researchers have discussed possible risks that might occur at any moment, conducted risk assessments at the university medical center, and designed emergency plans. As a result, a risk management plan for the healthcare sector on a worldwide scale was predicted. IT strategy assessments for healthcare institutions and their users were evaluated to detect sensitivities, risks, weaknesses, and concerns that affect the healthcare IT system in the risk assessment process. The identified threats have been assessed and controlled by presenting applicable control plans and suggestions to prevent or limit the potential risks in the healthcare system. The IT system can be developed and threats may be predicted in the future and controlled with good emergency plans based on field research and risk assessments [31].

Healthcare information systems (HIS) and security mechanisms for patient, institution, pharmacy, and health insurer data transfer were proposed by [32]. This is implemented by a comprehensive look at health information systems' existing security problems, as well as an introduction to Health Level 7 (HL7). Using HL7 communication issues as an example, researchers demonstrate how to conduct a simulated attack. An Autonomic Security Management plan was designed to secure a HIS against threats from both the inside and outside in a comprehensive manner. Real-time monitoring of a HIS' efficiency as possible, and the attack assessment function can forecast threats that might affect HIS operations. Research with security systems aimed at protecting the confidentiality and security of electronic health records has been reported. The ASM approach's attack control system identified the most suitable protective methods to restore the affected HIS to standard with little or no human interaction. It was concluded that the emerging software offered continuous real-time monitoring and control systems to evaluate effectively system risks, present security alerts, and protect the HIS from possible attacks by executing preventative measures. As a result, it can also identify and respond to threats that have avoided the system's security. To get the HIS back to normal, the best protections will be chosen based on their reliability [32].

A study by [33] examined the security of hospital systems in EU nations ranging from the medium to the low-income classes. An electronic anonymized questionnaire was used to collect data from ICT (information and communication technology) organizations and medical practitioners participating in the study. In 2019, a large healthcare in Portugal, a health clinic in Romania, and a health area in Greece all participated in the survey, with 53.6 percent and 6.71 percent clinical outcomes, respectively, for ICT and medical experts. The results show the need of establishing separate security organizations to evaluate facilities and behaviors, as well as the need for continual information security awareness initiatives. By analyzing the findings, researchers may better understand the actions taken at healthcare facilities and so enhance cybersecurity protection while lowering exposure to risk [33].

In a study, [34] analyzed healthcare data security to obtain a better grasp of current advances in health data security development. From 2005 to 2015, researchers conducted a 10-year study of articles published in Korean publications on "medical information." For each fiscal year, researchers also examined these journal publications, which were classified into two categories: literary research and empirical research, with additional divisions based on topics and issues. In the conclusion, 17 (35.4 percent) of these publications focused on rules, organizations, and programs, which was the most prevalent kind of study. Researchers discovered that articles on medical specialists were the most common in the literature, while studies of information security professionals and hospital professionals were the most common in empirical studies. Risk assessment in hospital information systems might improve from further study in terms of social perception, organizational development, and technological advancements, researchers suggested [34]. [35] Conducted an evaluation of international health vulnerabilities as part of the biological relation to risk management program. A multi-sectoral, interdisciplinary team of eight experts led to the evaluation process, which includes information assessments, interviews, focus groups, and on-site evaluations. The system's objective was to improve the strategic planning for Biological Threat Reduction programs (BTRP) and to provide quantitative assessment for monitoring partner countries' skills during BTRP participation. In over 25 countries, the approach has been used to develop a framework for identifying and assessing system-wide risk mitigation and management strategies, as well as performing periodic evaluations of their performance. According to the finding of this study, the adoption of a standard and comprehensive methodology has been effective for the identification of effective and sustainable initiatives focused on achieving both local as well as worldwide health security objectives [35].

In a study, [36] evaluated the risk evaluation at social protection facilities of Isfahan Province in the event of an emergency by using the healthcare quality index. The descriptive-analytical research was carried out in 2015 in Isfahan Province Social Insurance Healthcare facilities utilizing a cross-sectional approach. The Healthcare Quality Index Standardized Survey was performed to explore the risk evaluation. It was divided into two parts, one including basic information on health facilities and the other containing 145 indicators in systemic, operational, and developmental categories. Observations and interviews with the system's managers were used to complete the survey at each hospital. The approach of weighting was focused on the healthcare quality factor, which ranged from 0 to 2. Excel was used to examine the data. Findings from the safety index in the three examined healthcare institutions suggested that the security level in each of them was average. Although their condition is not serious, they need planning and management of important safety precautions, and these healthcare institutions required important short-term risk control strategies [36].

[37] Suggested a technique for conducting privacy impact assessments (PIA) and focuses on assessing organizational features and incorporates a set of well-defined indicators as input, proving its application to two health information systems with contrasting features. Using measurements and taking into consideration the unique characteristics of the organization, this research proposed a PIA technique. The system's effectiveness has been shown on two distinct health information systems. With the help of this tool, organizations may better assess the severity of possible cybersecurity threats and, as a result, choose the most effective security measure to protect the information they gather and store. Outcomes of the suggested PIA approach show that each security standard has been significant to the institution's data. To calculate the reliability level, the approach used takes into consideration the potential consequences of data privacy and security breaches on a given data collection, the weighting of each security standard, and the unique features of each organization. This indicated that the organization may make an accurate assessment regarding the security protections and privacy enforcement methods to adopt in order to appropriately protect its information based on the results of the PIA [37].

A study conducted by [38] evaluated healthcare information security risk assessments. This research was nearly done in 2014. There were 27 participants total, all of them were health service IT professionals. A survey with a variety of open and closed questions was used in the study. Test-retest correlation (r =0.78) was used to examine the accuracy of closed survey questions. The fire was found to be a significant risk factor for data security, according to the study's findings. Low-probability risk indicators included possible risks to people or the surrounding environment. Low-probability risk indicators included possible risks to people or the surrounding environment. The implementation of technological protections in healthcare institutions was the most common, contrasted to organizational and physical protections, according to the findings of the study. Immediate corrective steps have been needed to address high potential risk factors, according to the findings. As a result, the underlying problems of such threats must be found and addressed before any negative consequences may be experienced [38].

In a study, [39] discussed the current state of the art in assessing the cybersecurity threats associated with Supervisory Control and Data Acquisition systems (SCADA). Twenty-four approaches of risk assessment designed for or used in SCADA systems were selected and examined in depth. Afterward, researchers address the approaches' purpose, application area, phases of risk assessment targeted; major risk approaches addressed; impact assessment; resources of probability statistics; assessment, and tool assistance. An understandable classification scheme for SCADA cybersecurity evaluation models was proposed as a result of the analysis. In addition, researchers identified five research difficulties that face the area and suggest possible solutions. In spite of the fact that several risk assessment methodologies for SCADA systems are available, additional study and many improvements have been needed. To effectively manage the perspective organization level of the strategic planning of risk, overcome the attack, account for human factor and capture and formalization of professional opinion, and improve the safety of predictive information in information security risk assessment techniques for SCADA systems, improvements may be made [39].

A new interval type-2 fuzzy controller (IT2FIS) developed by [40] has been used to improve the risk assessment model for information technology. There are three sub-models that makeup IT2FIS, which include overall functionality, which is monitored by Functionalities, Motivation and Aiming; the possibility of an attack based on Security vulnerabilities; and at last the risk of an attack that is assessed by the possibility of an attack and the impact of an attack. Researchers were able to design and develop a comprehensive evaluation of information security risks by incorporating three sub-models. In spite of the fact that there is a lot of uncertainties in the records/knowledge/ knowledge about information technology, this technique will have an improved ability to anticipate risk analysis of data security despite the numerous risks caused by the consequences of illegal activities. Analyses of statistical data, adapted neuro-fuzzy inference system (ANFIS), and Multiple Linear Regression has been used to determine the model's reliability at the end. In each of the sub-cases, researchers have given some quantitative data analysis in order to demonstrate the validity of the system. For risk-informed judgments, the description of risk uncertainty to decision-makers is vital, and this research also acknowledges the relevance of this issue. In the future, the IT2F controller's hardware implementation may be studied. It is also possible to test the suggested controller's applicability for various real-time information security opportunists [40].

A healthcare information cybersecurity, security, and data threat assessment approach was evaluated by [41]. It is then compared to an infusion system application and examined to existing standards and practices to see whether it is feasible. Device-related hazards may be seen as part of one system, as shown by the analysis of frameworks. Security vulnerabilities in medical technology have been on the rise since the introduction of internet connections. This study presented an ISSP risk assessment methodology in order to protect health care facilities. As far as medical devices are concerned, regulatory agencies' best practices and standards tend to concentrate on either cybersecurity or personal security. These organizations seem to be primarily concerned with certifying safety-related procedures, and as a result, security risks that have a significant impact on patient health are mostly ignored. Standardized safety and protection risks may be evaluated using this framework, which helps determine the risk level and necessary procedures for securing medical devices. Since most healthcare device makers do not adhere to the Health Insurance Portability and Accountability Act (HIPAA) rules, the proposed model also offers a method for calculating privacy-related threats. The assessment and application of the suggested framework by FDA specialists should be the focus of future study since it will assist reduce healthcare industry risks [41].

In a research, [42] investigated the role of risk assessment in the management of work-related illnesses and injuries among hospital employees. The goal of this research had to find the best way to estimate healthcare risks. A comparison of the most often used approaches was performed. As many as there have been ways to measure patient care quality, none have been tailored to the unique challenges of hospital operations. This approach was adopted from the INCDPM (National Research and Development Institute for Labor Protection Bucharest) approach and also used to determine the standard associated risks for each employment post in each department, as well as the overall risk level for the health center as a whole. Risks in healthcare areas were higher than the average for all employees, but it does not surpass 3.50, which is considered a reasonable level of security for this kind of activity. The ELVIE approach was used to analyze the psychological hazards. In the future, procedures should be improved so that findings may be presented both numerically and graphically. It was concluded that the advantages of each technique varied. ELVIE and SOBANE procedures are simpler for executives and managers to understand than the INCDPM approach, which gives statistical results. In the future, procedures should be improved so that findings may be shown in both numerical and graphical form [42].

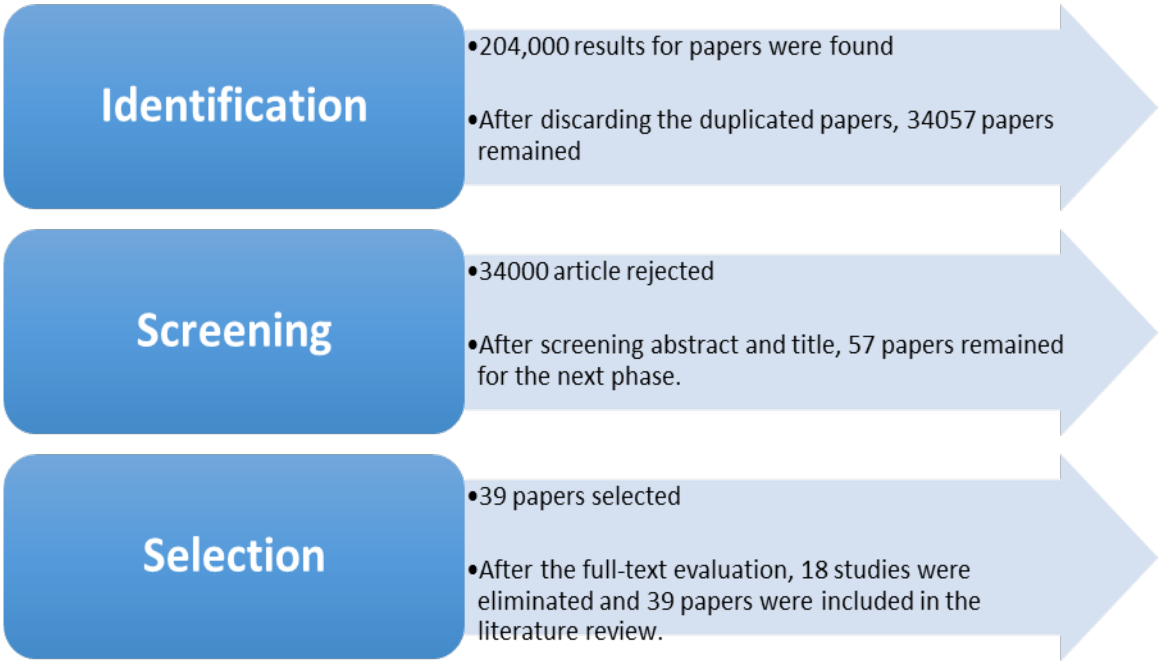
A system for risk analysis in health facilities was evaluated by [43]. To figure out what the users really want, researchers utilized a V system planning framework in combination with a variety of other methodologies, including as in-depth surveys and documentary reviews. To solve the present issues, it's important to provide specific information on risk assessment's basics. The approach researchers developed includes a risk assessment framework, explanatory cards, and a risk evaluation form to assist organize the risk assessment and recording the results, all of which are part of the framework. The framework was evaluated in various groups using a typical situation, and the results were utilized for user assessment. An interview-based user assessment was done with ten participants and provided positive findings. In addition to being used as a learning platform, the model was suggested for use in practice. Researchers expect that by incorporating it into risk assessments, people may arrive at better conclusions and take more suitable steps to reduce the risks they face. As a result, patient safety and quality of treatment might be enhanced [43].

In accordance with the ISO 31000 risk management concept, [44] assessed the tool's advantages and limitations. Stages in the Risk Management System include risk assessment, which identifies risks, analyses and evaluates all possible threats, and implements a risk management plan. The scientific method has developed a number of approaches for evaluating potential dangers. There are a number of various ways to analyze risk, and a risk assessment framework, also known as the "decision matrix risk assessment (DMRA) methodology," is one of the most used. Participants in the risk assessment process must address a wide range of topics, including the selection of the best methodological approach, determining the effectiveness of current control mechanisms, defining impact-consequences, describing risk probability scales, and creating a risk assessment matrix. With these concerns in mind, researchers have made many suggestions, which are particularly valuable when healthcare institutions don't provide enough information about risk assessments and how to respond to current issues [44].

3. RESEARCH METHODOLOGY

A systematic literature review method is employed in this study to offer a comprehensive analysis of previous papers and research in Security Risk Assessment in Medical Information Systems. The research design used in this study is qualitative and descriptive. I investigated some of the current risks associated with Medical Information Systems in particular. This research on the content and context of Medical Information Systems threats examines a wide range of Medical Information Systems-related vulnerabilities in more depth. An investigation of numerous sources was carried out in order to examine the Medical Information Systems vulnerabilities and establish whether or not these threats have an adverse effect on data security. According to the research design, scientific literature, as well as new articles from popular publications will be reviewed and analyzed in detail. A survey of the literature provides in-depth knowledge and understanding of this subject, Security Risk Assessment in Medical Information Systems. It gives context for the research and an overview of how the study relates to a broader field of research. The analysis of literature enables me to evaluate the sources that I used to conduct my research on Security Risk Assessment in Healthcare Information Systems.

The study was performed at the Purchase Public Library, which used online resources such as Google Scholar, Google Books, Microsoft Academic, Science.gov, PubMed Central, Research Gate, and other scientific databases to finish the study. Furthermore, I used the Google Chrome Browser to do research on security threats that were relevant to the subject of my study. Using specified search keywords, I conducted searches for scientific research and publications, as well as relevant articles. Among the relevant keywords I used were the following: *Data security risks in hospitals, Risk assessment, Cybersecurity risks, Information security threats, Medical data security vulnerabilities and Information security risk assessments in healthcare sector* keywords provided the most relevant results for this study.



Identification

- 204,000 results for papers were found
- After discarding the duplicated papers, 34057 papers remained

Screening

- 34000 article rejected
- After screening abstract and title, 57 papers remained for the next phase.

Selection

- 39 papers selected
- After the full-text evaluation, 18 studies were eliminated and 39 papers were included in the literature review.

Figure 1: Graphics for papers selection for literature review

The graphics for different steps of the selection of papers for literature review is shown in Figure 1. In the first step, 204,000 results for papers were found, after discarding the duplicated papers, 34057 papers remained. In the screening abstract and title, 34000 articles were rejected and 57 papers remained for the next phase. After the full-text evaluation, 18 studies were eliminated and 39 papers were included in the literature review. The distribution of chosen articles by year is shown in Figure 2. I noted that almost 80% of the papers were published between the years (2016-2022).

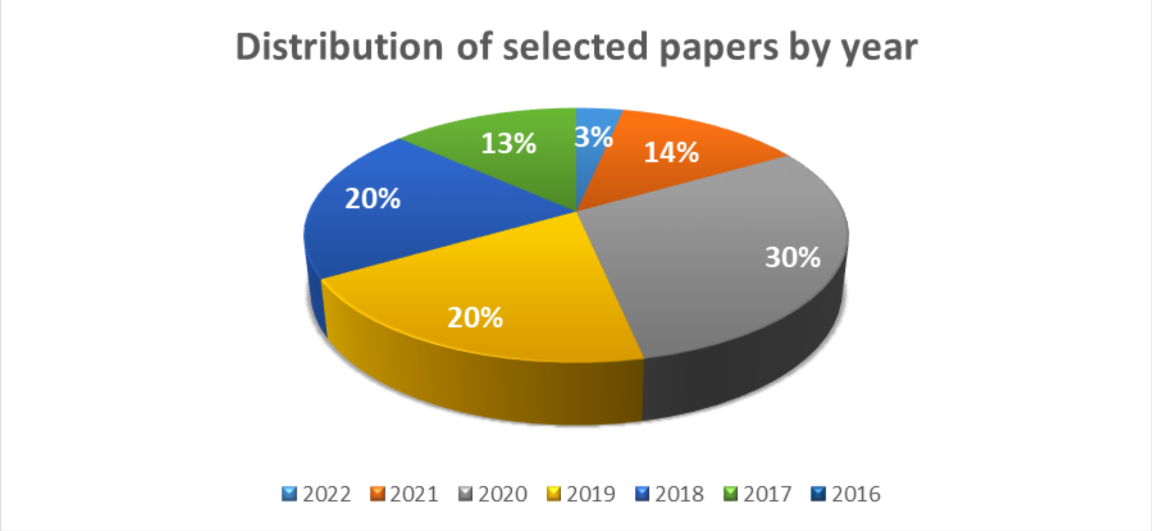


Figure 2: Distribution of selection papers by year

4. RESULTS AND DISCUSSION

This section will present and discuss the results of the literature review, and tables will summarize the risks and challenges. Additionally, the methodology, threats addressed, and suggested mitigations were included. Additionally, the publication years and authors of each research were listed. Additionally, the next part discusses the gap identified in the systematic review as well as future trends in risk assessment in medical information systems.

A notable concern raised in the literature was the refusal of most hospitals to employ information security risk management, which was a subject of discussion for the researchers [5-12]. Another key issue discussed in the literature was the lack of appropriate, robust security and privacy (S&P) in the healthcare system. This lack of security and privacy would threaten not just patients' privacy, but also their lives [16]. These vulnerabilities have the potential to result in a large number of issues with the cybersecurity of health information systems in the future, if not addressed immediately. Thus, the Ministry of Health should adopt effective strategies to strengthen the risk management of information security in healthcare facilities. S&P awareness among hospital information systems must be raised in future studies via the identification and quantification of possible S&P risks. Figure 3 shows the notable concerns in literature related risk assessments in hospital information security system, including the refusal of most hospitals to employ information security risk management (60%) and lack of security and privacy (40%).

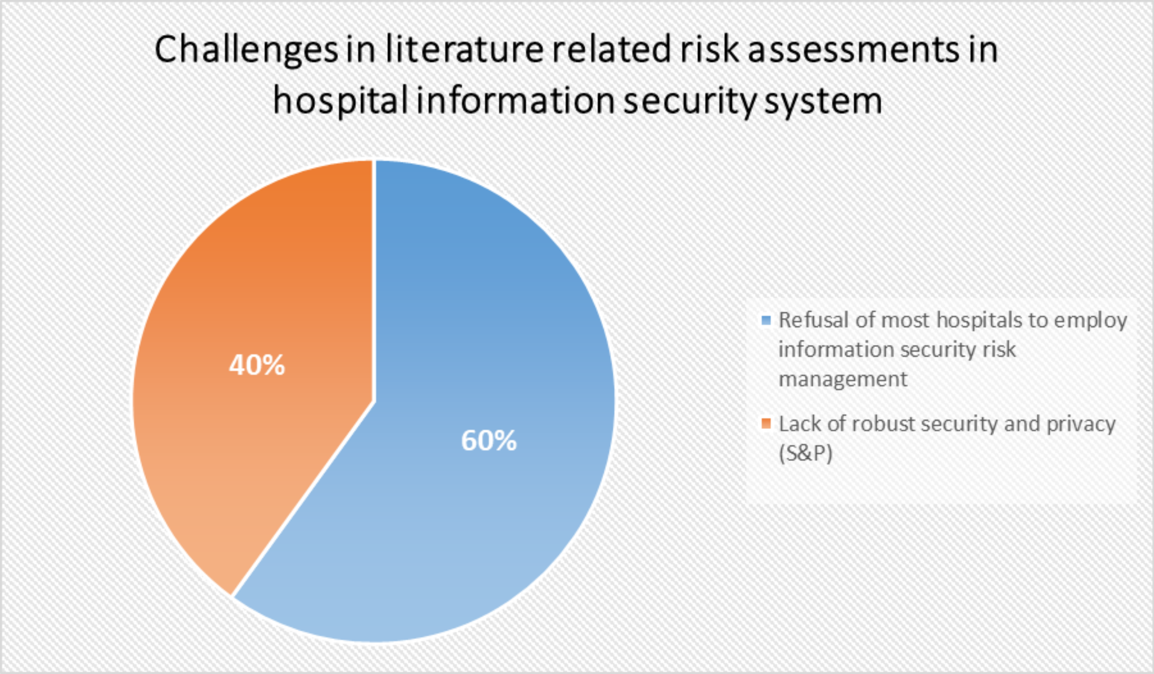


Figure 3: Challenges in literature related to risk assessment in hospital information security system

The following Table 1 summarizes the major threats and mitigations for information security risk assessment programs in the healthcare sector that have been identified by various research. In addition, the methodology was also mentioned according to each study. The findings indicated that the most often addressed problems and concerns about the cybersecurity of medical information systems were privacy concerns in the first place [20-28]. Furthermore, in medical information security systems, risks to patient data security, hardware, software, integrated technologies, and licenses were all prevalent [30-35].

Table 1: Summary Of Different Articles Evaluating Various Medical Security Threats

Title of article	Author	Publication year	Methodology	Addressed threats	Suggested mitigations
Information security risk management for computerized health information systems in hospitals: a case study of Iran	Zarei & Sadoughi	2016	Descriptive and cross-sectional research	Challenges of computerized health information systems (CHIS)	Information Security Risk Management (ISRM) program in hospital services
Security Control Model for Electronic Health Records	Kemboi & Ronoh	2021	A cross-sectional quantitative survey study design	Technical security threats, physical and administrative security threats	Data backup, temperature controls, and network services policies offer an organized system for implementing data security
Security Assessment of Information System in Hospital Environment	Tritilanunt & Surapol	2016	Quantitative research design	Hardware, software, integrated technologies, and licenses threats	Hospital IT Quality Improvement Framework (HITQIF)
Business continuity inspired fuzzy risk assessment framework for hospital information systems	Motevali Haghighi & Torabi	2020	Quantitative research	Hardware, software, human, network, database, and data warehouse risks	Business continuity-inspired fuzzy risk assessment framework (BC-FRA) for healthcare systems
Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment	Alsubaei & Shiva	2017	Quantitative research	Patients data threats, lack of proper security and privacy on internet of medical things (IoMT), less or no attention to devices, their interfaces, and applications addressed	IoMT taxonomy of security and privacy issues (S&P) proposed to increase the awareness
Evaluation of Hospital Information System of hospitals Affiliated to a University of Medical Sciences in West of Iran	Mirzaei et al.	2019	A cross-sectional quantitative survey study design	Risks related to medical staff, financial administration, health information management, and information technology	Creating web-based HIS capability, developing multilingual content for systems, and flexibility of software modules, purchasing software packages from software developer
Taxonomy of Information Security Risk Assessment	Shameli-Sendi et al.	2016	Quantitative, qualitative, hybrid	Vulnerabilities related to assets, medical services, business process	Developing information security risk assessment (ISRA)

(ISRA)					process and provide organizations with an awareness of the many risk assessment approaches available
Private Finance Initiative in the healthcare sector: trends and risk assessment	Akintoye & Chinyio	2005	Qualitative research	Security vulnerabilities in Private Finance Initiative (PFI)	Implementing a healthcare PFI research affects risks analysis, ultimate facility selection, or requirements
A study of future opportunities and challenges in digital healthcare sector: cyber security vs. Crimes in digital healthcare sector	Avani Rachh	2021	Quantitative and qualitative analysis	Vulnerabilities related to online transactions, digital healthcare system and information security	Develop security procedures at all levels to secure personal data and medical records, and increase awareness of data security
A Fuzzy Analytic Hierarchy Process for Security Risk Assessment of Web based Hospital Management System	Al-Mejibli & Alharbei	2019	Quantitative research	A healthcare web application's security vulnerability	Developing a fuzzy analytic hierarchy process with the purpose of increasing the usability and security of a healthcare web application
Risk Management Framework and Evaluation:Detail Site Study and Governance of Information Security Risk Management in Medical Information Technology Infrastructure in Hospitals	Divan et al.	2018	Qualitative research	Hardware, Software failures, and other vulnerabilities to medical system	Changing an ad-hoc network to one with a server (or wireless router) as a backbone
Global Health Security Risk Assessment in the Biological Threat Reduction Program	Kharaishvili et al.	2020	Qualitative research	International health vulnerabilities	strategic planning for Biological Threat Reduction programs (BTRP) for health security
Risk assessment in social security hospitals of Isfahan Province in case of disasters based on the hospital safety index	Tabatabaei & Abbasi	2016	A descriptive-analytical cross-sectional design	Technological, biological, societal, human-made, and hydro-meteorological threats	Implementing the necessary standards to increase safety and reduce damages

Integrated Security, Safety, and Privacy Risk Assessment Framework for Medical Devices	Yaqoob et al.	2020	Quantitative research	Hijacking, threats regarding device software, hardware, and batteries, as well as user interface issues	Adopting Integrated Safety, Security, and Privacy (ISSP) Risk Assessment Framework to evaluate the device's risk level and the security policies
Role of Risk Assessment in Prevention of Work-Related Accidents and Diseases in Hospital Staff	Boariu & Armean	2020	Quantitative research	Risks related to work-related illnesses and injuries among hospital employees	Adopting INCDPM, ELVIE and SOBANE approaches used to analyse the psychological and other healthcare hazards
A framework to support risk assessment in hospitals	Kaya et al.	2019	Mixed method	Healthcare risks and challenges with current risk assessment practice in hospitals	Implementing a risk assessment framework, explanatory cards, and a risk evaluation form to assist organize the risk assessment
Risk Analysis in Healthcare Organizations: Methodological Framework and Critical Variables	Pascarella et al.	2021	Mixed method	Patient safety risks and other healthcare vulnerabilities	Implementing risk matrix tool to identify the consequences level and risk rating

The following Table 2 shows the summary of different articles by evaluating cybersecurity risks, including different addressed threats and suggested mitigations for information security risks assessment programs in healthcare sectors. In addition, the methodology was also mentioned according to each study. The findings revealed that cyber-attacks, medical device hijacking, ransomware, and other criminal activities were the most often addressed problems and concerns with medical information systems [15-22].

Table 2: Summary of different articles evaluating cybersecurity risks

Title of article	Author	Publication year	Methodology	Addressed threats	Suggested mitigations
IoT a security risk management model for healthcare industry	Salih et al.	2019	Qualitative research	Cyber-attacks, medical device hijack and ransomware in hospitals	The formulation of IoT Security Risk Management Model for Healthcare based on DEMATEL procedure
A review of cyber security risk assessment methods for SCADA systems	Cherdantseva et al.	2016	Quantitative research	Cyberattacks	Implement SCADA (Supervisory Control and Data Acquisition) technologies to ensure cyber security

Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security	Jana & Ghosh	2018	Quantitative research	Cybersecurity vulnerabilities and other criminal actions	Implementing a unique type-2 fuzzy logic inference system model for cybersecurity evaluation improvements
A Risk Assessment Framework Proposal Based on Bow-Tie Analysis for Medical Image Diagnosis Sharing within Telemedicine	Poleto et al.	2021	Quantitative research	Cybersecurity risks	Adopting risk evaluation frameworks expected to enable bow-tie assessment to recognize possible risks in information security and act preventatively, detecting the causes
A Cyber Security Risk Assessment of Hospital Infrastructure including TLS/SSL and other Threats	Millar	2016	Quantitative research	Cyber threats	Improve significant reforms in national health service (NHS) to elevate cyber security to a top priority without affecting the NHS's long-standing commitment to medical safety
A New Methodology for Information Security Risk Assessment for Medical Devices and Its Evaluation	Mahler et al.	2020	Quantitative research	Cybersecurity risks	Implementing a threat identification, likelihood, severity decomposition, and risk integration technique (TLDR) based on ontologies for improving security
Security risk assessment in Internet of Things systems	Nurse et al.	2017	Qualitative research	Cybersecurity risks	Adopting novel approaches and best practices for risk analysis need to take into account the dynamic nature of the Internet of Things (loTs

The following Table 3 shows the summary of different articles by evaluating the data privacy breaches and other security vulnerabilities, including different addressed threats and suggested mitigations for information security risks assessment programs in healthcare sectors. In addition, the methodology was also mentioned according to each study. The results showed that the most tackled issues and concerns with data privacy breaches and other security vulnerabilities in medical information systems was the HIPPA data breaches, external hackers, staff carelessness, or non-compliance with security standards and medical information leakage in the first place [30-39].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3: Summary of different articles evaluating the data privacy breaches and other security vulnerabilities

Title of article	Author	Publication year	Methodology	Addressed threats	Suggested mitigations
Creating a Standardized Risk Assessment Framework Library for Healthcare Information Technology	Schmeelk	2020	Qualitative research	Data breaches, Web application vulnerabilities	Developing a Standard Risk Evaluation Conceptual model Libraries for Hospital information technology and risk assessment process
Information security climate and the assessment of information security risk among healthcare employees	Kessler et al.	2020	Quantitative research	HIPPA data breaches, external hackers, staff carelessness, or non-compliance with security standards and procedures	Information Security Climate Index (ISCI) for risk assessment and awareness
Health Information Security in Hospitals: the Application of Security Safeguards	Mehraeen et al.	2016	Quantitative research	Information security and data protection issues due to lack of guidelines for resolving security concerns, and an absence of well-documented policies	Administrative, technical, and physical safeguards for data security. Implementing security rules, network management strategies, and user training are suggested.
Towards Autonomic Security Management of Healthcare Information Systems	Chen & Lambright	2016	Qualitative research	Internal and external attacks on healthcare information system	Integrate with the HL7 standard and the Autonomic Security Management (ASM) strategy for attack mitigation
A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures	Gioulekas et al.	2022	Quantitative research	A healthcare information security vulnerabilities	Information security systems and software (e.g., antivirus databases, UTM firewalls with IDS/IPS) should be upgraded
Trends in Research on the Security of Medical Information in Korea: Focused on Information Privacy Security in Hospitals	Kim et al.	2018	Quantitative research	Medical information leakage and other medical accidents	Regulations and government programs such as HIPPA and others recommended

Utilizing a privacy impact assessment method using metrics in the healthcare sector	Makri et al.	2020	Quantitative research	Data privacy breaches	Suggested a privacy impact assessment (PIA) technique for determining security and privacy enforcement solutions
Information Security Risk Assessment in Hospitals	Ayatollahi & Shagerdi	2017	Mixed-method	Threats to hospital information and computer security, physical/environmental threats	Implementation of early-warning fire, cooling, and smoke detection systems
A Markov-Based Model for Information Security Risk Assessment in Healthcare MANETs	Das et al.	2019	Quantitative research	Information security breaches	Implementing MISRAM is a best mitigation strategy for Risk Management of Data Security in Hospital
Security analysis and improvement of bio-hashing based three factor authentication scheme for telecare medical information systems	Jiang et al.	2018	Quantitative research	Threat of exposing sensitive medical information to illegal entities	Implementing 3FA scheme's compliance with both data encryption privacy and secure authentication standards
Security Risk Assessment in Electronic Health Record System	Madhavi & Lincke	2018	Quantitative research	Risks of data breaches associated with electronic Health Records (EHRs)	Implementing a strategy to evaluate the cybersecurity risks to determine rates of cyberattack types and quantify SLE (Single Loss Expectancy)

Figure 4 shows the addressed threats in literature related risk assessments in hospital information security system. The findings of the results show the hardware, software failures, and other vulnerabilities (15%), technical security threats, physical, management and other administrative security threats (7%), data privacy breaches (7%), risks related to work-related injuries among hospital employees (7%), overall cybersecurity vulnerabilities and other criminal actions (25%), data privacy breaches and other security vulnerabilities (39%).

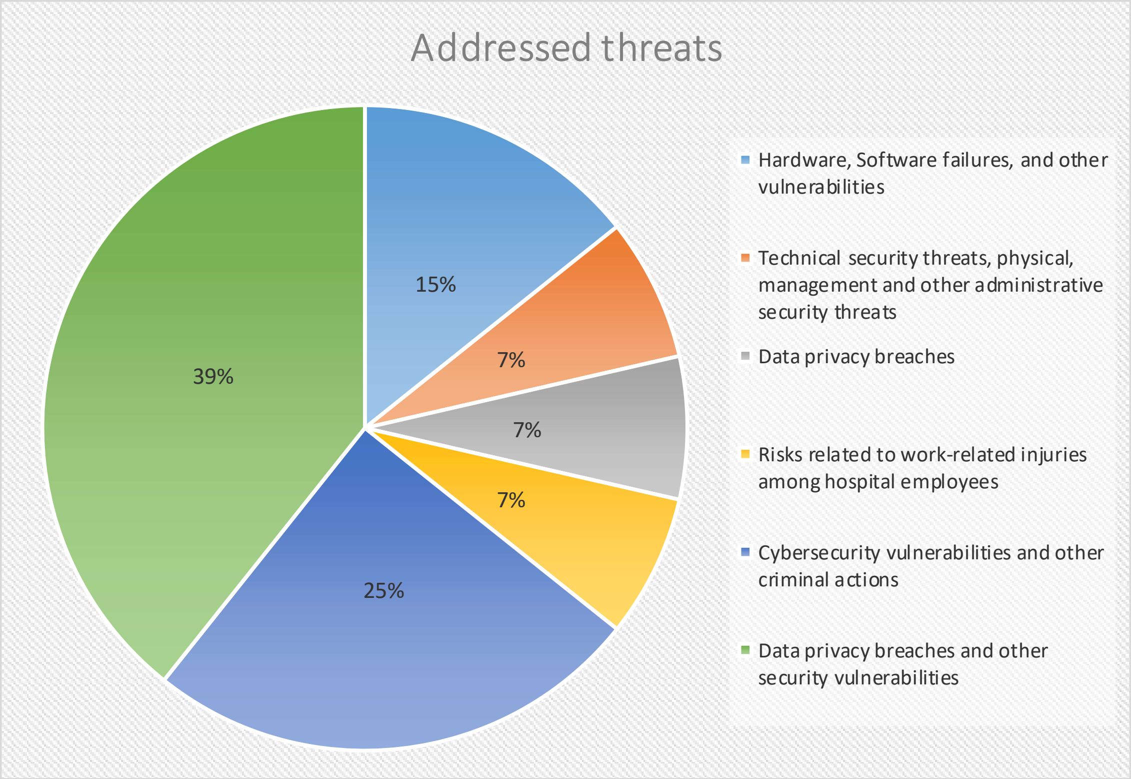


Figure 4: Addressed threats in literature

Figure 5 shows the suggested mitigations in literature related risk assessments in hospital information security system. According to the findings of results, the suggested mitigations for a secure information security system in hospitals include implementing information security risk management program in hospital services (34%), implementing security rules (15%), data backup, temperature controls, and network services policies (5%), developing multilingual content for systems, and flexibility of software modules (5%), provide awareness related risk assessment approaches (20%), suggested strategic planning for biological threat reduction programs (5%), improve significant reforms in national health service (NHS) to elevate cyber security (5%), recommendations of regulations and government programs such as HIPPA (10%) and others (1%).

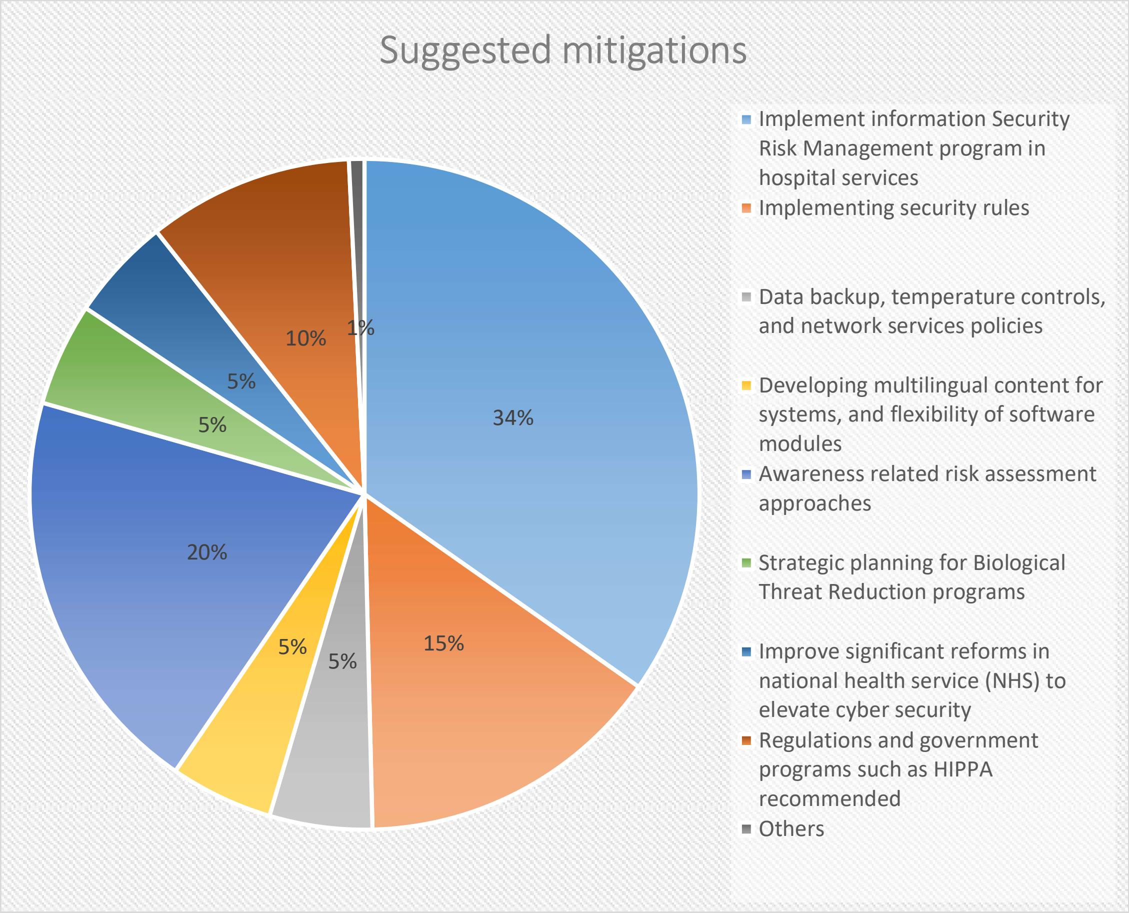


Figure 5: Suggested mitigations in literature

Figure 6 shows the methodology used in literature. According to the findings of results, the literature involved Descriptive and cross-sectional research (3%), Quantitative research design (69%), Quantitative-qualitative or hybrid research (6%), Qualitative research design (22%).

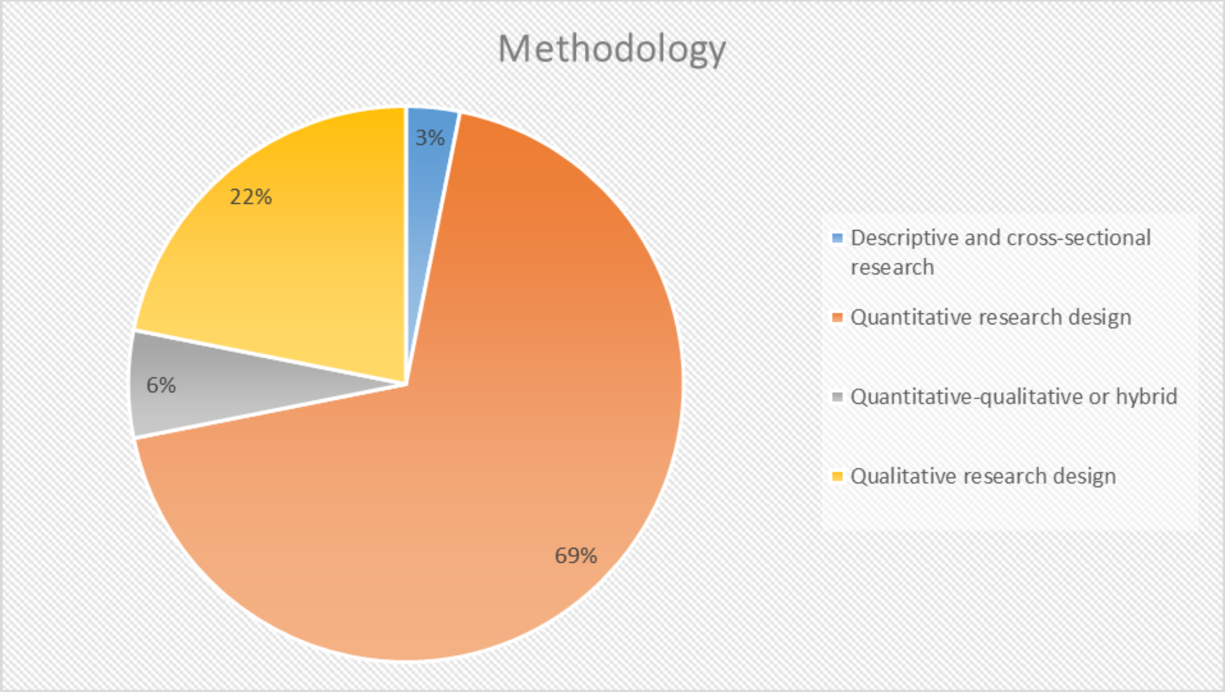


Figure 6: Methodology used in literature

5. CONCLUSION

This study used a systematic evaluation of the literature to provide an in-depth examination of previous studies and research on Security Risk Assessment in Medical Information Systems. A wide range of Health Information Systems (HIS) risks was examined in more detail in this study on the complexities of threats to Medical Information System. A further contribution of this study is that it includes tables that explain the methodology, risks addressed, and possible mitigations for a number of studies, which increases the relevance of the research. In the literature, there were two prominent points of concern: the refusal of most hospitals to implement information security risk management and the lack of suitable, robust security and privacy (S&P) measures in the healthcare system. Patients' privacy and security would be affected as a result of this lack of security and privacy, which might even put their lives at risk. If these risks are not addressed soon, they have the potential to lead to a significant number of challenges with the security of healthcare information systems in the future. So the Ministry of Health should implement efficient techniques to improve the risks management of information security in healthcare organizations. The focus of this study is mostly on assessing medical information system security concerns and mitigating these risks via the efforts. Healthcare organizations may use the results of the research to enhance IT efficiency and patient data security. By highlighting the threats involved with information security, the study will encourage people to secure themselves. It covers the strategies that hospitals have implemented to strengthen their data security and patient identification techniques in order to better serve their patients.

6. ACKNOWLEDGMENT

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Research No. Grant No. 6039).

RFERENCES:

[1] Ayatollahi, H., & Shagerdi, G. (2017). Information Security Risk Assessment in Hospitals. The Open Medical Informatics Journal, 11(1), 37–43. https://doi.org/10.2174/1874431101711010037

[2] Chen, Q., Lambright, J., & Abdelwahed, S. (2016). Towards Autonomic Security Management of Healthcare Information Systems. Proceedings - 2016 IEEE 1st International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE 2016, 113–118. https://doi.org/10.1109/CHASE.2016.58

[3] Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. Sensors, 22(2), 572.

[4] Almaiah, M. A., & Al-Khasawneh, A. (2020). Investigating the main determinants of mobile cloud computing adoption in university campus. Education and Information Technologies, 25(4), 3087-3107.

[5] Al Nafea, R., & Almaiah, M. A. (2021, July). Cyber security threats in cloud: Literature review. In 2021 international conference on information technology (ICIT) (pp. 779-786). IEEE.

[6] Almaiah, M. A., Hajjej, F., Ali, A., Pasha, M. F., & Almomani, O. (2022). A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS. Sensors, 22(4), 1448.

[7] Adil, M., Khan, R., Ali, J., Roh, B. H., Ta, Q. T. H., & Almaiah, M. A. (2020). An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment. IEEE Access, 8, 163209-163224.

[8] Adil, M., Almaiah, M. A., Omar Alsayed, A., & Almomani, O. (2020). An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. Sensors, 20(8), 2311.

[9] Akour, I., Alnazzawi, N., Alshurideh, M., Almaiah, M. A., Al Kurdi, B., Alfaisal, R. M., & Salloum, S. (2022). A Conceptual Model for Investigating the Effect of Privacy Concerns on E-Commerce Adoption: A Study on United Arab Emirates Consumers. Electronics, 11(22), 3648.

[10] Siam, A. I., Almaiah, M. A., Al-Zahrani, A., Abou Elazm, A., El Banby, G. M., El-Shafai, W., ... & El-Bahnasawy, N. A. (2021). Secure health monitoring communication systems based on IoT and cloud computing for medical emergency applications. Computational Intelligence and Neuroscience, 2021.

[11] Almaiah, M. A., Ali, A., Hajjej, F., Pasha, M. F., & Alohali, M. A. (2022). A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. Sensors, 22(6), 2112.

[12] Khan, M. N., Rahman, H. U., Almaiah, M. A., Khan, M. Z., Khan, A., Raza, M., ... & Khan, R. (2020). Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks. IEEE Access, 8, 176495-176520.

[13] Alabadleh, A., Aljaafreh, S., Aljaafreh, A., & Alawasa, K. (2018). A RSS-based localization method using HMM-based error correction. Journal of Location Based Services, 12(3–4), 273–285.

[14] Almaiah, M. A., Al-Zahrani, A., Almomani, O., & Alhwaitat, A. K. (2021). Classification of cyber security threats on mobile devices and applications. In Artificial Intelligence and Blockchain for Future Cybersecurity Applications (pp. 107-123). Cham: Springer International Publishing.

[15] Adil, M., Khan, R., Almaiah, M. A., Al-Zahrani, M., Zakarya, M., Amjad, M. S., & Ahmed, R. (2020). MAC-AODV based mutual authentication scheme for constraint oriented networks. IEEE Access, 8, 44459-44469.

[16] Almomani, O., Almaiah, M. A., Alsaaidah, A., Smadi, S., Mohammad, A. H., & Althunibat, A. (2021, July). Machine learning classifiers for network intrusion detection system: comparative study. In 2021 International Conference on Information Technology (ICIT) (pp. 440-445). IEEE.

[17] Adil, M., Khan, R., Almaiah, M. A., Binsawad, M., Ali, J., Al Saaidah, A., & Ta, Q. T. H. (2020). An efficient load balancing scheme of energy gauge nodes to maximize the lifespan of constraint oriented networks. IEEE Access, 8, 148510-148527.

[18] Alsyouf, A., Lutfi, A., Al-Bsheish, M., Jarrar, M. T., Al-Mugheed, K., Almaiah, M. A., ... & Ashour, A. (2022). Exposure detection applications acceptance: The case of COVID-19. International Journal of Environmental Research and Public Health, 19(12), 7307.

[19] Bubukayr, M. A. S., & Almaiah, M. A. (2021, July). Cybersecurity concerns in smart-phones and applications: A survey. In 2021 international conference on information technology (ICIT) (pp. 725-731). IEEE.

[20] Almaiah, M. A. (2021). A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In Artificial intelligence and blockchain for future cybersecurity applications (pp. 217-234). Cham: Springer International Publishing.

[21] Schmeelk, S. (2020). Creating a standardized risk assessment framework library for healthcare information technology. Proceedings of the Annual Hawaii International Conference on System Sciences, 2020-January, 3881–3890. https://doi.org/10.24251/hicss.2020.474.

[23] Zarei, J., & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: A case study of Iran. Risk Management and Healthcare Policy, 9, 75–85. https://doi.org/10.2147/RMHP.S99908.

[24] Almaiah, M. A., Almomani, O., Alsaaidah, A., Al-Otaibi, S., Bani-Hani, N., Hwaitat, A. K. A., ... & Aldhyani, T. H. (2022). Performance investigation of principal component analysis for intrusion detection system using different support vector machine kernels. Electronics, 11(21), 3571.

[25] Almaiah, M. A., Dawahdeh, Z., Almomani, O., Alsaaidah, A., Al-Khasawneh, A., & Khawatreh, S. (2020). A new hybrid text encryption approach over mobile ad hoc network. Int. J. Electr. Comput. Eng.(IJECE), 10(6), 6461-6471.

[26] Alrawad, M., Lutfi, A., Alyatama, S., Elshaer, I. A., & Almaiah, M. A. (2022). Perception of occupational and environmental risks and hazards among mineworkers: A psychometric paradigm approach. International journal of environmental research and public health, 19(6), 3371.

[27] Almaiah, M. A., Al-Rahmi, A., Alturise, F., Hassan, L., Lutfi, A., Alrawad, M., ... & Aldhyani, T. H. (2022). Investigating the effect of perceived security, perceived trust, and information quality on mobile payment usage through near-field communication (NFC) in Saudi Arabia. Electronics, 11(23), 3926.

[28] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. Electronics, 11(20), 3330.

[29] Albalawi, A. M., & Almaiah, M. A. (2022). Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. J. Theor. Appl. Inf. Technol, 100, 2988-3011.

[30] Kemboi, L., & Ronoh, L. (2021). Security Control Model for Electronic Health Records. International Journal of Applied Sciences: Current and Future Research Trends, 12(1), 43-52.

[31] Al-Mejibli, I. S. (2019). A Fuzzy Analytic Hierarchy Process for Security Risk Assessment of Web based Hospital Management System. International Journal of Advanced Trends in Computer Science and Engineering, 8(5), 2470–2474. https://doi.org/10.30534/ijatcse/2019/92852019

[32] Alsubaei, F., Abuhussein, A., & Shiva, S. (2017). Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. Proceedings - 2017 IEEE 42nd Conference on Local Computer Networks Workshops, LCN Workshops 2017, September 2018, 112–120. https://doi.org/10.1109/LCN.Workshops.2017.72.

[33] Qasem, M. H., Obeid, N., Hudaib, A., Almaiah, M. A., Al-Zahrani, A., & Al-Khasawneh, A. (2021). Multi-agent system combined with distributed data mining for mutual collaboration classification. IEEE Access, 9, 70531-70547.

[34] Almudaires, F., & Almaiah, M. (2021, July). Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation. In 2021 International Conference on Information Technology (ICIT) (pp. 732-738). IEEE.

[35] AlMedires, M., & AlMaiah, M. (2021, July). Cybersecurity in industrial control system (ICS). In 2021 International Conference on Information Technology (ICIT) (pp. 640-647). IEEE.

[36] Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., ... & Alghanam, O. A. (2023). Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using sem. Sustainability, 15(13), 9908.

[37] Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., & Alrawad, M. (2023). A new blockchain-based authentication framework for secure IoT networks. Electronics, 12(17), 3618.

[38] Mohamed, M. A., Shawai, Y. G., Almaiah, M. A., Derahman, M. N., Lutfi, A., & Bakar, K. A. A. (2024). Challenges in data representation for efficient execution of encryption operation. Bulletin of Electrical Engineering and Informatics, 13(2), 1207-1216.

[39] Scientific, L. L. (2024). ENHANCING CLOUD SECURITY BASED ON THE KYBER KEY ENCAPSULATION MECHANISM. Journal of Theoretical and Applied Information Technology, 102(4).

[40] ALKHDOUR, T., ALMAIAH, M. A., ALI, A., LUTFI, A., ALRAWAD, M., & TIN, T. T. (2024). REVOLUTIONIZING HEALTHCARE: UNLEASHING BLOCKCHAIN BRILLIANCE THROUGH FUZZY LOGIC AUTHENTICATION. *Journal of Theoretical and Applied Information Technology*, *102*(4).

[41] ALMAIAH, M. A., ALI, A., SHISHAKLY, R., ALKHDOUR, T., LUTFI, A., & ALRAWAD, M. (2024). A NOVEL FEDERATED-LEARNING BASED ADVERSARIAL FRAMEWORK FOR AUDIO-VISUAL SPEECH ENHANCEMENT. *Journal of Theoretical and Applied Information Technology*, *102*(4).

[42] ALMAIAH, M. A., ALI, A., SHISHAKLY, R., ALKHDOUR, T., LUTFI, A., & ALRAWAD, M. (2024). BUILDING TRUST IN IOT: LEVERAGING CONSORTIUM BLOCKCHAIN FOR SECURE COMMUNICATIONS. *Journal of Theoretical and Applied Information Technology*, *102*(3).

[43] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms. *Sensors*, *24*(2), 713.

[44] Jalil, M., Ali, N. H., Yunus, F., Zaki, F. A. M., Hsiung, L. H., & Almaayah, M. A. (2024). Cybersecurity Awareness among Secondary School Students Post Covid-19 Pandemic. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *37*(1), 115-127.