World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

Health information systems security: Risks, prospects and frameworks

Henry Mathews Odiango *, Silvance Abeka and Samuel Liyala

Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya.

World Journal of Advanced Engineering Technology and Sciences, 2022, 06(02), 057–070

Publication history: Received on 13 June 2022; revised on 17 July 2022; accepted on 19 July 2022

Article DOI: https://doi.org/10.30574/wjaets.2022.6.2.0082

Abstract

Information is the most precious asset of any organization and assessing risk to information is a core mandate of any institutional management to ensure availability of effective controls to protect information assets. The increasing digitization of health information and the ever-changing cyber security threat environment, has led to some public health data breaches and as information security become increasingly important to the continued success for businesses, majority of organizations are searching for an appropriate security framework. Security risk assessment framework enables identification of threats and vulnerabilities. Although numerous frameworks available in the market, selection of the right framework to meet the organization's need is a challenge due to lack of prescriptiveness, standard, inconsistencies, complexity, compliance, cost, and certifications. To address the gap, this study assessed the security of health information system and privacy risks in addition to existing frameworks and developed an enhanced framework. The study adopted a descriptive cross – sectional design and was conducted in Siaya County, in Kenya. A questionnaire was used to collect data which was analyzed and presented inform of tables, and charts. The results indicated that confidentiality of information is good (use of identifiers and passwords at 96.8% approval rate), availability of physical controls to protect authorized access at 95.2%, availability of policies stating staff responsible for protection of information confidentiality at 91.9%, availability of written policy on patient confidentiality and privacy at 74.2% and use of access privileges at 68.8%. The findings on integrity of information was poor with availability of systems to review data accuracy having 71.9% approval rate, frequency of data review at 81.2%, availability of written description of information security manager's responsibility at 39.5%, monitoring of electronic systems to detect potential breaches at 40%, creation of audit logs to track system transactions at 54% and frequency of reviewing audit logs at 51.5%. The findings on availability of information was good (availability of inventory of computers at 69.9%), regular updates of inventory at 61.3%, updates of patient data on laptops and desktops at 68.2%, sharing of data confidentiality and security policy at 36%, and regular backups of audited logs at 51% approval rates. Regarding the assessment of existing security frameworks, it was noted that HIPAA has the following shortcomings: lacks complete valid risk analysis, not certifiable, security rule is safeguarding electronic protected health information only, the security does not regulate emails and does not require encryption, and commitment on security is verbal. On the other hand, ISO/IEC 27001 is expensive, requires specific IT budget, special expertise, and more time to apply in public hospitals. Finally, NIPP framework is expensive, and uses consequence's assessment which is outside the scope of this study.

Keywords: HIS; ePHI; NIPP; HIPAA; Risks; Security

1. Introduction

In a typical scenario, patients may seek treatment from numerous hospitals during their lifetime. Consequently, they leave scattered healthcare records in different hospitals. The implications are that accessing previous healthcare records belonging to these patients presents some uphill challenges. According to [1], these fragmented records result

*Corresponding author: Henry Mathews Odiango
Jaramogi Oginga Odinga, University of Science and Technology, Bondo, Kenya.

in poor management of patient data. It is also possible for each of these hospitals to have its own healthcare record management software. Therefore, there is lack of networking among the health service providers which imply scattered healthcare records in diverse disconnected places [2]. As explained in [3], devoid of integrated data management coupled with isolated healthcare record from medical labs, insurance firms and pharmaceutical manufacturers result in the breakdown of health information across providers. However, the rapid development of information technology has facilitated the development of Telecare Medicine Information System (TMIS) [4] as well as Health Information Systems (HISs). These systems comprise of medical sensors [5], smart robotics and smart phones that help patients in remote locations to access health care services. Using TMIS, it has become possible for doctors to utilize robots and smart digital sensor to carry out surgeries [6], [7]. In addition, authors in [8] explain that technology integration in the healthcare industry has seen the conversion of paper-based health records to electronic records. The goals of this conversion may include enhanced productivity and efficiency in healthcare facilities. It also makes it possible for the electronic personal health information (ePHI) to be easily accessible, permitting global health networking.

The continued adoption of HISs has led to the enhancement of accessibility, efficiency and quality of healthcare services. It has also resulted in reduced medical errors, better healthcare, increased efficiency and accuracy of patient care and administration [9]. According to [10], secure and scalable data sharing is critical for healthcare decision-making system. However, the traditional fragmented healthcare record systems impede effective information flow and hence prevent patients from making sensible treatment decisions. On the other hand, TMIS enables the patient from any remote location to contact the hospital medical server to share and access required information over some public channels [11]. As explained in [12], TMIS has made it possible for patients to access doctor's telemedicine services over the internet. In so doing, TMIS accelerate the convenience of healthcare services access to patients at their place of preference [13], providing real-time remote diagnosis. As discussed in [14], these digital healthcare technologies have revolutionized the healthcare sector, enabling efficient collection, storage and access to ePHI.

Although TMIS, HIS andePHI have numerous advantages, they are faced by many challenges. For instance, large volumes of private and sensitive patient data is stored in TMIS which can result in grave consequences if maliciously accessed or leaked [15]. This calls for safe storage, transmission as well as the reservation of integrity in these TMIS [16], [17]. As discussed in [4] and [18], TMIS has various setbacks such as false authentication, key losses, and failure of the data node that brings forth serious loss of data. Therefore, security and privacy are key for the safe transmission and storage of electronic patient records [19], [20], [21], [22], [23].

The identity authentication process of TMIS occurs in a public channel, which is vulnerable to attackers. Attackers can disrupt the authentication process through eavesdropping, interception, and forgery method, and launch malicious attacks such as forgery attacks, replay attacks, and side-channel attacks [24]. These attacks can lead to malicious access, data loss and intellectual property infringement [25]. During the development and implementation of TMIS and HIS, privacy and security should be incorporated in early stages [26], [27]. In addition, interoperability between healthcare systems should be assured so that there is efficient exchange of health records between providers [28]. During internet-facilitate diagnosis and treatment, many threats can be launched to the exchanged messages over the open internet [29]. In addition, the design of new systems to address security and privacy challenges in digital healthcare record systems must uphold interoperability, secure transfer, storage, and efficient retrieval [30]. This will help healthcare breaches vectors such as Worms, Trojan horse, computer viruses, hacking and ransomware [31]. However, ensuring the security of massive personal health information (PHI) being collected by numerous electronic devices has been noted to be cumbersome [32]. As such, the assurance of perfect confidentiality, integrity, secrecy and security in TMIS remains challenging [13].

To prevent resource abuse and malicious attacks, authentication [33] is normally the first step. Here, the TMIS need to validate the identities of all network entities before access is granted. Additional security measure such as antivirus, encryption, firewalls, audit logs, usernames and passwords can also be implemented. Moreover, legislative and regulatory frameworks can be implemented in healthcare facilities to enhance security. For instance, based on the Health Insurance Portability and Protection Act (HIPAA), healthcare providers need to put in place standards and policies to govern the security and protection of electronic health and medical information. Failure to comply with personal data protection legislation, healthcare facilities may face civil and legal penalties [14]. In the long run, such non-compliance may cause some harm to the employees or patients [34].

2. Related work

Many threats, attacks, risks and vulnerabilities lurk in TMIS, HIS and ePHI systems. For instance, author in [35] has identified distributed denial of service (DDOS), privilege escalation, phishing, spoofing and password guessing attacks as being frequent and consequential in healthcare organizations. In addition, malware, worms, spyware, viruses, trojans,

ransomware, rootkits, adware and sniffers have been found to be serious issues in the healthcare sector. Moreover, hazards such as tornados, floods and fires may destroy health information and systems [36]. As explained in [37], attacks and threats against hospitals, medical devices and healthcare entities are on the rise. Here, the threat agent utilize techniques such as phishing, botnets, man-in-the-middle [38] and SQL injections to exploit various vulnerabilities in hospital systems, networks. These vulnerabilities may be in software applications, system security procedures, regulatory compliance, policies and procedures [14]. The motivation behind these attacks range from financial gains to political gains.

To curb these attacks and threats, security frameworks have come up with security control mechanisms that all healthcare facilities need to adopt in order to thwart, detect or minimize vulnerabilities, attacks and threats against their electronic healthcare systems. The three pillars for securing HIS systems comprise of administrative, physical and technical security controls [39], [40]. The administrative controls may include security policies, staff training, rules and procedures for assigning access to HIS, maintenance of audit trails, methods for incident reporting as well as accountability and disciplinary actions for violation of policies [41]. On the other hand, physical security controls encompasses proper device disposal, device isolation and emergency contingency protocols [42]. On their part, technical security controls include biometrics, access control systems [43], passwords, encryption, antivirus, firewalls, radio frequency identification (RFID) and Intrusion Detection System (IDS) [44]. According to [45], healthcare organizations and hospitals subscribe to healthcare legislations that are regulated by the concerned jurisdiction. These regulations and legislations offer the groundwork for enhanced and resilient healthcare systems. In this regard, various techniques have been put forward to protect HIS as well as the data exchanged in TMIS.

To provideinteroperability and secure way to store and exchange information, blockchain technology (BT) has been adopted [46]. Here, BT helps in the maintenance of patient electronic health records (EHRs) and electronic medical records (EMRs) for numerous telemedicine, medical devices, and billing systems. The deployment of public blockchain serves to minimize the requirement for dependable nodes during information exchanges [47]. As pointed out in [48], privacy safeguards must be incorporated in any blockchain architecture employed to build healthcare applications. In HIS, BT can be utilized to offer data consistency of the health record [49]. This serves to enhance quality, facilitate patient and physician coordination and hence improve the overall outcome. BT can also permit patient-centric control of healthcare data sharing among the healthcare facilities [50]. Essentially, it acts as a clinical data repository that offers distributed ledger record of all medical events. By so doing, it permits healthcare providers to have seamless access to patient electronic health records [1]. This helps address the traditional fragmented healthcare record keeping issues where access to this data presents some challenges especially when the patient is in critical condition. To enhance data management, several blockchain based workflows for the healthcare environment have been designed in [51]. Similarly, blockchain medical record storage and sharing systems have been designed in [52] and [53], while patient-centric healthcare data management system has been developed in [54] for storage and privacy enhancement. On the other hand, blockchain-based apps for healthcare have been presented in [55]. However, blockchain has high storage and computation complexities [56].

Another important technology for healthcare security enhancement is the physically unclonable function (PUF), which generates unique and unpredictable response data for any challenge information [57]. For instance, an access control and authentication scheme in [4] combines PUF and Elliptic Curve Cryptography (ECC) to ensure the safety of TMIS. Similarly, the verification scheme in [58] incorporates PUF in its design. However, this scheme cannot withstand secret disclosure and de-synchronization attacks [59]. In addition, a PUF based privacy protection access control scheme is developed in [60], while a lightweight access control protocol is introduced in [18]. However, PUF-based schemes have stability issues [61]. Moreover, the protocol in [18] can potentially expose the identity information of the tag and hence is susceptible to traceability attacks. Apart from PUF, intrusion detection systems can also help secure HIS. For instance, a secure identity authentication and intrusion detection scheme is presented in [62], while an ECC based access control protocol is introduced in [63]. Similarly, lightweight and secure authentication protocols are developed in [64] and [65]. However, identity based schemes have key escrow issues [66], while the scheme in [63] offers only a one-way verification function. On its part, the protocol in [64] is vulnerable to packet replays, identity and password guessing attacks.

An efficient, secure and robust protocol has been presented in [67]. Unfortunately, this protocol is vulnerable to traceability, stolen smart card, privileged insider, packet replays, server impersonation, identity and password guessing attacks [68], [69]. On the other hand, an access control and key establishment protocol is presented in [70]. Although this scheme has low authentication costs, it cannot withstand replay attacks [71]. In addition, the password cannot be updated correctly. Based on chaotic maps, a novel authentication protocol is developed in [72]. However, this protocol cannot offer both untraceability and anonymity [73]. As such, an improved scheme is presented in [73]. Unfortunately, this enhanced protocol cannot withstand stolen smart card attacks [74]. To prevent man-in-the-middle and replay

attacks, a three-factor access control protocol is developed in [75]. However, this scheme is still vulnerable to simulation and internal attacks [76]. On the other hand, a radio frequency identification scheme has been developed in [77] that is shown to be lightweight and secure. This scheme is shown to resist forgery, de-synchronization, replay and denial of service attacks. Unfortunately, for the scheme in [77], the real identities are exchanged in plaintext between the tag and its reader [78]. On the other hand, a digital signature based technique is presented in [79] for securing transaction history of the patient, while an RSA based authentication scheme is presented in [80]. However, this technique has lower efficiency due to the utilization of modulo exponentiation operations. Based on chaotic maps, secure remote access control methods are introduced in [81] and [82]. However, chaotic map based protocols are susceptible to stolen smart-card, impersonation, identity and password guessing attacks [27]. In addition, the approach in [81] cannot withstand side-channel attacks, while the technique in [82] is vulnerable to offline password guessing and impersonation attacks [83]. Similarly, a patient-centric data sharing system is developed in [84] based on machine learning algorithms for anomaly detection.

To offer string location confidentiality in healthcare system, an efficient access control scheme is presented in [85]. However, this technique is vulnerable to replay and random nonce exposure attacks. An access control technique is introduced in [86] to offer database and reader authentication so as to thwart sever loss attacks. However, this approach fails to offer anonymity as well as protection against both replay and asynchronous attacks [87]. On the other hand, secure and efficient protocol is introduced in [88] to secure telemedicine services. Unfortunately, this scheme is inefficient due to massive message exchanges during session key derivation. To address these issues, a secure and efficient authentication protocol is developed in [89], while another new design for telemedicine services protection is developed in [90]. Unfortunately, these two protocols are vulnerable to stolen card information, identity and password guessing attacks. To secure private data in healthcare sector, a scheme based on secondary residue and timestamp is presented in [87]. This technique is shown to withstand replay attacks. However, it fails to protect against asynchronous attacks and it also incurs high implementation costs. This is detrimental to cost constrained [91] TMIS system components such as medical sensors. To address this, an efficient authentication method is developed in [92]. Although the scheme in [93] offers mutual authentication, it is susceptible to replay attacks [94]. This problem is addressed by the El-Gamal cryptographic system developed in [95]. On the flip side, this approach incurs high storage costs [96].

A telecare medicine information systems presented in [97] has a number of vulnerabilities that were addressed by the scheme developed in [98]. However, the technique in [98] is vulnerable to man-in-middle, offline password guessing, user and server impersonation attacks. To share medication history in a secure and efficient way, authors in [99] have developed a public key based method. However, the usage of this public key infrastructure may lead to high overheads [100]. On the other hand, an authentication protocol for remote healthcare systems is introduced in [101]. Unfortunately, this method is vulnerable to session-specific temporary information attack [102]. Although the protocol developed in [103] is efficient and secure, it cannot provide anonymity and is susceptible to impersonation and password guessing attacks [104], [105]. This anonymity challenge is addressed by the PUF based scheme developed in [106]. Based on RFID, a privacy preservation protocol is presented in [107] securing remote medical data. However, this approach cannot withstand de-synchronization, denial of service and replay attacks. To solve these issues, an identity-based remote user authentication scheme is developed in [108]. Unfortunately, this approach is vulnerable to stolen verifier, impersonation and secret key leakage attacks [109]. In addition, it has some key escrow [110] issues. Although the scheme in [102] solves some of these challenges, it is shown to be susceptible to password guessing, impersonation and session key hijacking attacks [111]. To uphold security among the involved entities in the TMIS, two schemes are developed in [112] and [113]. However, these two protocols cannot withstand stolen verifier and cloning attacks.

In light of the above HIS security and privacy challenges, this paper sought to develop an enhanced framework for assessing HIS security and privacy risk.

3. Tools and methods

The study was conducted in six public hospitals in Siaya County and it adopted a descriptive cross – sectional research design. It basically involved the assessment of the existing HIS security and privacy risks which facilitated the development of a framework for assessing HIS security and privacy risk. The sample was established through proportionate stratified random sampling technique. The target population was Technical staff from the six public hospitals. The Yamane model was used to determine the study's sample size from the target population. It has a confidence level of 95%. The study sample was 61 participants picked purposively in order to get the needed information. Mathematically, this model is represented as follows:

$$n_s = \frac{N}{\{1+N(e^2)\}}$$

Where:

n_s - Sample size
N - Population size
e - Precision level (at 0.92 confidence interval, e = 0.08)
Given N = 100, then:

$$n_s = \frac{100}{\{1+100(0.08)^2\}} = \frac{100}{\{1+100(0.0064)\}} = \frac{100}{1.64} = 60.97 \cong 61 \text{ Participants}$$

The study population comprised technical staff working in the six public hospitals especially from the units that generate, process, store, analyses and disseminate the Health Information. Siaya County has 10 public health hospitals and this study focused on six of the public hospital that is 60%. Table 1 presents the proportionate stratified sampling that was adopted.

Table 1 Proportionate Stratified Sampling

Stratum	Population	Sample size	As a % (proportion) of 61
Siaya County Referral Hospital	25	15	24
Yala Sch	15	9	15
Bondo Sch	20	12	19
Madiany Sch	10	7	12
Ukwala Sch	15	9	15
Ambira Sch	15	9	15
Total	100	61	100

Data collection was through structured questionnaire with both open and closed ended questions which was administered with an aid of research assistants in face-to-face interviews with respondents. The data collection instruments were piloted in two hospitals (Uyawi and Rwambwa) which were not involved in the study, the results were used to perfect the instruments and improve the quality output. Regarding validity and reliability, this study focused on two types of validity, first was the content validity which assessed whether the instrument adequately covered all the content that it should cover with respect to the variables. Content validity was determined by the pilot conducted in two hospitals that were not included in the survey. The second validity was Face validity which is the extent to which a tool appears to measure what it is supposed to measure. This was confirmed by the expert opinion. Completed questionnaires were coded and data entry and analysis done using statistical package for social sciences (SPSS V.20). Data was summarized using frequencies, percentage, means and standard deviation. Results are presented in form of charts and tables.

4. Results and discussion

A total of 64 questionnaires were completed. Higher proportion of the respondents 36(56.2%) were male and 28(43.8%) were female. More than half 40 (62.5%) were aged between 20 and 30 years old and 22(34.4%) were Health records and information officers. More than half 40 (62.5%) had diploma as highest level of professional training.

Based on the research findings majority of the respondents were Health Records and Information Officers at 22(34.4%), followed by Nurses, at 16(25%), Clinical officers at 14(21.8%), Environmental Health at 5(7.8%), then pharmacist at 4 (6.3%), Nutritionists at 3.1%, and last but not least medical doctors at 1.6%. The finding indicates that Health Records and Information Officers are the majority when it comes to issues with Information security since that is their main responsibility in terms of Health Management Information Systems (HMIS).

4.1. Health Information Systems Security and Privacy Risks

This section analyzed data on the security and privacy of the Health Information system by focusing on the information confidentiality, information integrity and information availability. Majority of the respondents 55(85.9%) agreed to use computer to perform their duties as shown in Fig.1.

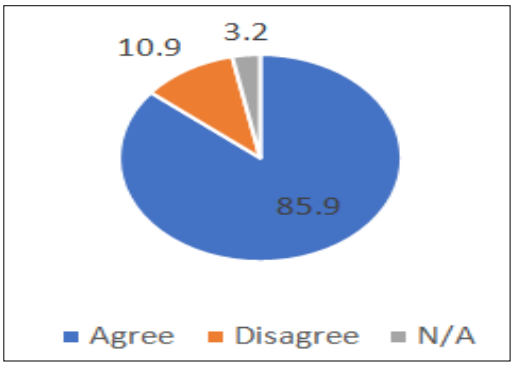

Figure 1 Use computer to perform duties

Among the 55 that use computer to perform their duties, higher proportion used the computers for data entry (94.1%), sending reports (93.8%), report writing (87.2%) and for data analysis (81.4%). Smallest proportion of the respondents (44.8%) used computer for entertainment as shown in Fig.2.

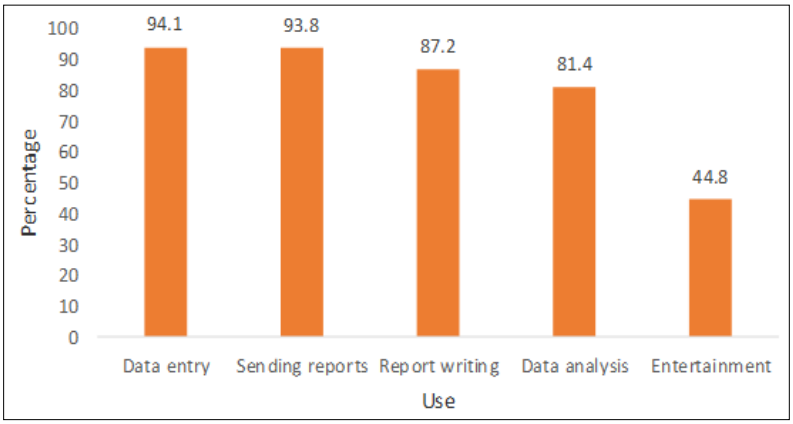

Figure 2 Computer Applications Scenarios

4.1.1. Information confidentiality

The respondents were asked to indicate the level of information confidentiality applied in the six-sub county hospital's Health information systems. Majority of the respondents agreed that staff need a user identifier and password to gain access to a computer (96.8%, n = 60), computers permitted to be connected to more than one network (85.2%. n = 52), policies state that staff is personally responsible for protecting paper records, computer workstations, laptop computers associated with confidential information (91.9%, n = 59), written policy available for ensuring the confidentiality, security and privacy of personally identifiable health data (74.2%, n = 46), The facility is using emails, flash discs, intranet, external hard disk, file transfer protocol, optical media and smart card in transferring electronic data within a site, (77.4%, n = 48). The facility is using access privileges, encryption Antivirus security to protect information during transmission, (68.8%, n = 42). Facility is using Physical measures for protecting patient privacy while collecting information (85.8%, n = 54) and that Physical security control's in place to prevent unauthorized access to buildings and rooms containing personally identifiable health data (95.2%, n = 57). On average, they agreed with the statements on information confidentiality (mean 1.8, SD 0.1).

4.1.2. Information Integrity

The respondents were asked to indicate the extent to which information integrity is applied in the six-sub county hospital's Health information systems. Majority of the respondents agreed that all persons authorized to access

personally identifiable health data trained on the organization's information security policies and procedures (69.8%, n = 44), on the other hand availability of clearly defined roles to all persons with authorized access to personally identifiable data (78.1%. n = 50), on the availability of a designated information security manager at the facility (57.8%, n = 37) meanwhile ,only (39.5% , n = 24) agreed that a written description of the information security manager's responsibilities available. Majority of respondents (71.9 %, n = 46) agreed that system to review data accuracy in the facility available, while more than half (64.1%, n = 42) agreed that documented processes for handling data inaccuracies are available, and on whether electronic systems are monitored to detect potential or actual security breach less than half agreed (40%, n = 26). Slightly more than half agreed that audit logs are created to assist in recording all system transactions (54%, n=34). Majority agreed that Data is reviewed frequently for accuracy (81.2%, n= 52), half of the respondent's agreed that audit logs are reviewed frequently (51.5%, n = 33), while only (38.3%, n =24) agreed that risk assessments conducted in their facilities, (27.5%, n = 17) agreed that risk assessment is conducted monthly in their facilities, and (26.6%, n = 17) agreed that the following methods are used to conduct risk assessment: threat identification, vulnerability assessment, control analysis, likelihood determination, impact analysis and risk determination. The integrity of data according to the results is low with the least being on risk assessment.

4.1.3. Information Availability

The study sought to establish the level of information availability across the six sub county hospitals in Siaya County.Majority of the respondent's agreed that Facility has updated inventory of computers and mobile devices containing personally identifiable health data (69.9%, n = 44). Inventory of computers and mobile devices records are updated regularly (61.3%, n = 38), while the statement that patient data on desktop and laptop are updated frequently (68.2%,n=43) Data Confidentiality and Security Policy shared with patients (36%, n = 23). Facility audit logs are backed up regularly (49.2%, n = 43) and on whether data on desk top and laptop are backed up, regularly (64.5%, n = 40), Audit logs are backed up regularly (51% n = 28).

4.1.4. Frameworks for Assessing Health Information Systems Security and Privacy Risks

This section presents the results of the assessment of different security frameworks that exist and being used by various organizations worldwide.

HIPAA - The Health Insurance Portability and Accountability Act was enacted to create uniformed formats and rules to covered entities regarding electronic health transmissions. These rules required the development of specific regulation, including standards for electronic transactions, privacy of individually identifiable health information, national employer identification, security, national provider identification, and proposed enforcement rule.

ISO/IEC 27001 Framework - ISO/IEC 27001 being international standard for information security management enable organization to identify security risks and set controls in place to manage and eliminate them, win stakeholder and customer trust since they trust that their confidential data is well protected, the ISO/IEC 27001 framework help keep information assets secure and aid organization manage the security of assets such as employee details, intellectual property, financial information.

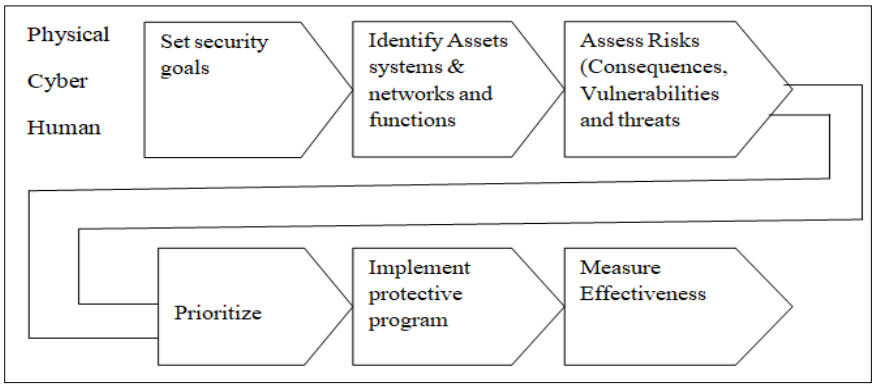

Figure 3 Adopted from National Infrastructure Protection Plan- Risk Management framework

National Infrastructure Protection Plan- Risk Management framework -The main focus of NIPP-RM framework is to identify key systems, assets, networks, and functions highly in need of focused risk mitigation measures this risk management, principle combining consequence, vulnerability, and threat information aid continuous improvement. The current information of each part is looked at against the baseline information captured and analyzed at initial risk

assessments to evaluate progress. This process enables a feedback loop, to monitor progress and implement actions to enhance protection and stability of, the physical, cyber, and human components in every process of the risk management frame.As shown in Fig.3, the national infrastructure protection plan risk management framework (NIPP-RM) is structured to promote continuous improvement to enhance critical infrastructure protection and key resource protection.

A whole consequence assessment takes into consideration economic, psychological, public health and safety, and government impacts; however, estimating potential indirect impacts needs the use of assumptions and more complex variables. An assessment of complete categories of consequence is outside the scope and capabilities available for a given risk analysis. At a minimum, assessments should focus on the two most fundamental impacts: the human and the most relevant direct economic impact.

4.2. Enhanced Framework for Assessing HIS Security and Privacy Risk

A framework for assessing security risk of an information system must entail comprehensive picture of the available security risk and assist in offering options and alterations to the security measures and controls. Based on this, this study postulates that none of the assessed three frameworks is holistically providing expected outcome.Therefore, this paper advances the opinion that an enhancement is required which will improve the security risk assessment process, and that enhancement can be made to include three more components which will be added and placed as process (see Fig.4).

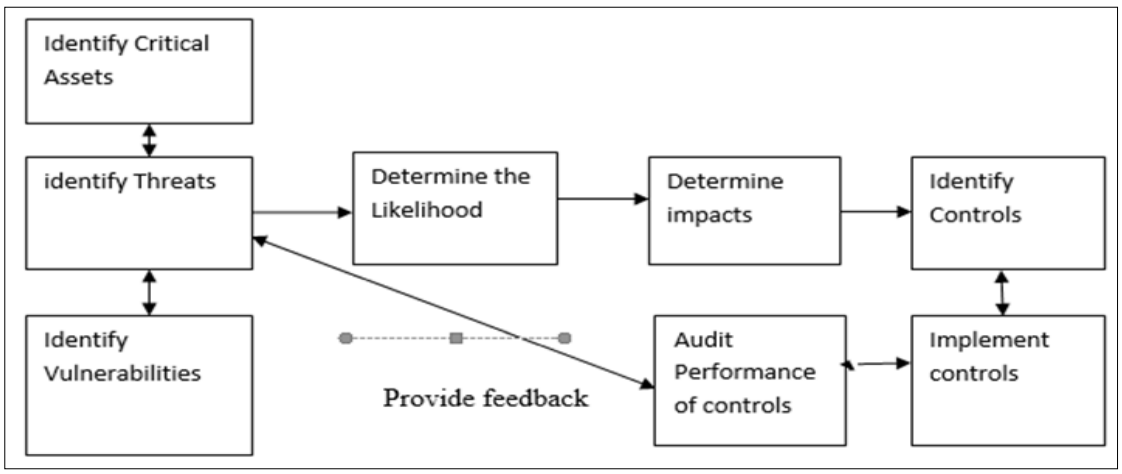

Figure 4 Proposed Enhanced Framework

4.2.1. Identify likelihood

Since likelihood of an event exploiting vulnerability is a core measurement in the process of risk assessment which help produces a rating for each asset.

4.2.2. Determine impacts

Certain impact has the ability to trigger several catastrophic events like the loss of data, damage to laptops and computers, but other impacts may have negligible effect on an institution. A valid wholesome impact analysis looks into factors such as: impact to the organization's mission, the systems, and data, besides, this analysis needs to consider the sensitivity and criticality of the data and the system.

4.2.3. Provide feedback

Currently, information technology infrastructure is dynamic. So, continuous feedback of security risks and functionality of controls provide accountability of changes to business requirements and priorities, and also new threats and vulnerabilities are detected at an early stage and nipped before it is late.

5. Conclusion

Based on the study findings, it is concluded that security of health information systems and privacy risk in the six public Hospitals is in place and among the three CIA Triad: protection of information confidentiality is leading based on i)

availability of policies indicating that staff are responsible for protecting paper records, computer work stations, and laptops with data .ii) Written policies available to ensure confidentiality security and privacy of personally identifiable health data iii) use of access privileges like encryption, antivirus to protect information during transmission ,iv) use of identifier and passwords to gain access to computers v) the use of physical security controls to prevent unauthorized access to buildings and rooms containing personally identifiable health data . In general, the finding on information confidentiality had a mean of 1.8, SD 0.1, and overall, the information confidentiality in the six hospitals is good. However, the study found that there are practices that breach information confidentiality such as connecting computers and laptops to more than one network, sharing of electronic devices while transferring electronic data form laptops and desktop. The study revealed that Information integrity in the six public Hospitals is poor based on the following i) all persons authorized to access personally identifiable health data are trained on the organization's information security policies and procedures, the score was slightly above average ii) availability of clearly defined roles to all persons with authorized access to personally identifiable data, not all the hospital have this in place .iii) System to review data accuracy is not available in all the six hospitals assessed. The study finding indicates the following variables to be the worst in terms of promoting information integrity, iv) availability of a designated information security manager at the facility, v) availability of written description of information security manager's responsibilities only, and electronic systems are monitored to detect potential and/or actual security breach, less than half agreed (40%, n = 26) vi) creation of audit logs to track all system transactions in the health facility, slightly more than half agreed on its availability , while half of the respondents agreed that vii) audit logs are reviewed frequently . In regards to risks assessments, the result indicates less than 40% agreed that risk assessments conducted in their facilities, the finding points to a major weakness in the fight against information insecurity and also indication that the information security within the six hospital is at risk. Less than 30% agreed that Risk assessment is conducted Monthly and the same percentage agreed that risk assessment is conducted using the following methods; threat identification, vulnerability assessment, Control analysis, Likelihood determination, impact analysis and Risk determination. Information security could be estimated and assessed by doing risk analysis and evaluation. The outcome can assist in planning information security requirements and risk control measures. Information availability According to study findings, availability of information in the six Public hospitals is good based on the following i) updating inventory of computers and mobile devices with personally identifiable health data at (69.9%, n = 44) aid in tracking location of computers and monitor for any potential threat to information, ii) The frequency of updating inventories of computers and mobile devices at (61.3%, n = 38 help identify threats and likelihood of computers being at risk to information damage or loss, iii) updating patient data on desktop and laptop, at (68.2%, n = 43) help prevent information loss, duplication, deletion by mistake, virus attack, mixed up even lost. iv) Data Confidentiality and Security Policy shared with patients which scored (36%, n = 23) show poor practice since Patients should be informed on the confidentiality and availability of their data to win their trust and v) audit logs are backed up regularly, at (51%, n = 28) this is not good since backing up information is a secure way of maintaining availability of information in case something interferes with the original storage. On average the information availability in the six facilities had (a mean of 2.6, SD 0.1). From the study findings it can be concluded that the information security frameworks assessed which includes (HIPAA, ISO/IEC 27001 and NIPP- RM), did not meets the standards desired for a simple, easy to use and re-adjustable framework that covers the most important components of an information security requirement that follow the right procedure and addresses the most fundamental elements of a framework, it is in this basis this study has proposed an enhanced framework.

Compliance with ethical standards

Acknowledgments

We would like to acknowledge our colleagues who provided us with any support that saw the successful completion of this paper.

Disclosure of conflict of interest

The authors hereby declare that they do not have any conflict of any interest.

References

[1] Chelladurai U, Pandian S. A novel blockchain based electronic health record automation system for healthcare. Journal of Ambient Intelligence and Humanized Computing. 2022 Jan; 13(1):693-703.

[2] Mead CN. Data interchange standards in healthcare it-computable semantic interoperability: Now possible but still difficult. do we really need a better mousetrap?. Journal of Healthcare Information Management. 2006 Jan 1;2 0(1):1–21

[3] Houlding D, MSc CI. Health information at risk: successful strategies for healthcare security and privacy. Healthcare IT Program Of ce Intel Corporation, white paper. 2011, 1-8.

[4] Xiao L, Xie S, Han D, Liang W, Guo J, Chou WK. A lightweight authentication scheme for telecare medical information system. Connection science. 2021 Jul 3; 33(3):769-85..

[5] Nyangaresi VO, Ogundoyin SO. Certificate Based Authentication Scheme for Smart Homes. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[6] Javed AR, Beg MO, Asim M, Baker T, Al-Bayatti AH. Alphalogger: Detecting motion-based side-channel attack using smartphone keystrokes. Journal of Ambient Intelligence and Humanized Computing. 2020 Feb 15: 1-14.

[7] Sarwar MU, Javed AR. Collaborative health care plan through crowdsource data using ambient application. In2019 22nd international multitopic conference (INMIC) 2019 Nov 29 (pp. 1-6). IEEE.

[8] Zeng X. The impacts of electronic health record implementation on the health care workforce. North Carolina medical journal. 2016 Mar 1; 77(2):112-114.

[9] Ngafeeson MN. Healthcare information systems opportunities and challenges. Encyclopedia of Information Science and Technology, Third Edition. 2015:3387-3395.

[10] Siyal AA, Junejo AZ, Zawish M, Ahmed K, Khalil A, Soursou G. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography. 2019 Jan 2; 3(1):3.

[11] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In 2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[12] Kumar V, Ahmad M, Kumari A. A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS. Telematics and Informatics. 2019 May 1; 38:100-17.

[13] Shamshad S, Ayub MF, Mahmood K, Kumari S, Chaudhry SA, Chen CM. An enhanced scheme for mutual authentication for healthcare services. Digital Communications and Networks. 2022 Apr 1; 8(2):150-61.

[14] Chuma KG, Ngoepe M. Security of electronic personal health information in a public hospital in South Africa. Information Security Journal: A Global Perspective. 2022 Mar 4; 31(2):179-95.

[15] Amin R, Islam SH, Gope P, Choo KK, Tapas N. Anonymity preserving and lightweight multimedical server authentication protocol for telecare medical information system. IEEE journal of biomedical and health informatics. 2018 Sep 14; 23(4):1749-59.

[16] Kui X, Feng J, Zhou X, Du H, Deng X, Zhong P, Ma X. Securing top-k query processing in two-tiered sensor networks. Connection Science. 2021 Jan 2; 33(1):62-80.

[17] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Sep; 3(5):1-16.

[18] Liang W, Xie S, Zhang D, Li X, Li KC. A mutual security authentication method for RFID-PUF circuit based on deep learning. ACM Transactions on Internet Technology (TOIT). 2021 Oct 22; 22(2):1-20.

[19] Song J, Zhong Q, Wang W, Su C, Tan Z, Liu Y. FPDP: flexible privacy-preserving data publishing scheme for smart agriculture. IEEE Sensors Journal. 2020 Aug 18; 21(16):17430-8.

[20] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. In International Conference on Internet of Things as a Service 2022 (pp. 3-18). Springer, Cham.

[21] Wang W, Huang H, Zhang L, Su C. Secure and efficient mutual authentication protocol for smart grid under blockchain. Peer-to-Peer Networking and Applications. 2021 Sep; 14(5):2681-93.

[22] Javed AR, Sarwar MU, Beg MO, Asim M, Baker T, Tawfik H. A collaborative healthcare framework for shared healthcare plan with ambient intelligence. Human-centric Computing and Information Sciences. 2020 Dec; 10(1):1-21.

[23] Zhang L, Zou Y, Wang W, Jin Z, Su Y, Chen H. Resource allocation and trust computing for blockchain-enabled edge computing system. Computers & Security. 2021 Jun 1; 105:102249.

[24] Nyangaresi VO. ECC based authentication scheme for smart homes. In2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[25] Liang W, Fan Y, Li KC, Zhang D, Gaudiot JL. Secure data storage and recovery in industrial blockchain network environments. IEEE Transactions on Industrial Informatics. 2020 Jan 13; 16(10):6543-52.

[26] Justinia T. Blockchain technologies: opportunities for solving real-world problems in healthcare and biomedical sciences. Acta Informatica Medica. 2019 Dec; 27(4):284.

[27] Dharminder D, Kumar U, Gupta P. A construction of a conformal Chebyshev chaotic map based authentication protocol for healthcare telemedicine services. Complex & Intelligent Systems. 2021 Oct; 7(5):2531-42..

[28] Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: preserving security and privacy. Journal of big data. 2018 Dec;5(1):1-8.

[29] Nyangaresi VO. Provably Secure Protocol for 5G HetNets. In 2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[30] Burghard C. Big data and analytics key to accountable care success. IDC health insights. 2012 Oct; 1:1-9.

[31] Hummelholm A. Future Smart Societies' Infrastructures and Services in the Cyber Environments. In Cyber Security 2022 (pp. 151-182). Springer, Cham.

[32] Beck EJ, Gill W, De Lay PR. Protecting the confidentiality and security of personal health information in low-and middle-income countries in the era of SDGs and Big Data. Global health action. 2016 Dec 1; 9(1):32089.

[33] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Jun 25:100210.

[34] Asija R, Nallusamy R. A survey on security and privacy of healthcare data. In Conference Paper· July 2014 Jul.

[35] Conaty-Buck S. Cybersecurity and healthcare records. Am Nurse Today. 2017; 12(9):62-4.

[36] Pankomera R, van GREUNEN D. Mitigating vulnerabilities and threats for patient-centric healthcare systems in low income developing countries. In 2017 IST-Africa Week Conference (IST-Africa) 2017 May 30 (pp. 1-11). IEEE.

[37] Bernard R, Bowsher G, Sullivan R. Cyber security and the unexplored threat to global health: a call for global norms. Global Security: Health, Science and Policy. 2020 Jan 1; 5(1):134-41.

[38] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. In International Conference for Emerging Technologies in Computing 2021 Aug 18 (pp. 3-20). Springer, Cham.

[39] Kruse CS, Smith B, Vanderlinden H, Nealand A. Security techniques for the electronic health records. Journal of medical systems. 2017 Aug; 41(8):1-9.

[40] Ives TE. The New'E-Clinician'guide to compliance. Audiol. Today. 2014; 26(1):52-3.

[41] Andriole KP. Security of electronic medical information and patient privacy: what you need to know. Journal of the American College of Radiology. 2014 Dec 1; 11(12):1212-6.

[42] Wanyonyi, E., Rodrigues, A., Abeka, S., &Ogara, S. Effectiveness of security controls on electronic health records. International Journal of Scientific & Technology Research. 2017 Jan; 6(12): 47–53.

[43] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In 2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[44] Lemke, J. Storage and security of personal health information. Ontario Occupational Health Nurses Association Journal. 2013 Jun; 32(1):25-6.

[45] Marutha N. The application of legislative frameworks for the management of medical records in Limpopo Province, South Africa. Information Development. 2019 Sep; 35(4):551-63.

[46] Panigrahi A, Nayak AK, Paul R. HealthCare EHR: A Blockchain-Based Decentralized Application. International Journal of Information Systems and Supply Chain Management (IJISSCM). 2022 Jul 1; 15(3):1-5.

[47] Abdellatif AA, Al-Marridi AZ, Mohamed A, Erbad A, Chiasserini CF, Refaey A. ssHealth: toward secure, blockchain-enabled healthcare systems. IEEE Network. 2020 Apr 22; 34(4):312-9.

[48] Kavathekar SS, Patil R. Data Sharing and Privacy–Preserving of Medical Records Using Blockchain. InInternational Conference on Sustainable Communication Networks and Application 2019 Jul 30 (pp. 65-72). Springer, Cham.

[49] Zhang P, Walker MA, White J, Schmidt DC, Lenz G. Metrics for assessing blockchain-based healthcare decentralized apps. In2017 IEEE 19th international conference on e-health networking, applications and services (Healthcom) 2017 Oct 12 (pp. 1-4). IEEE.

[50] Gordon WJ, Catalini C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Computational and structural biotechnology journal. 2018 Jan 1; 16:224-30.

[51] Khatoon A. A blockchain-based smart contract system for healthcare management. Electronics. 2020 Jan 3;9(1):94.

[52] Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec: Using blockchain for medical data access and permission management. In2016 2nd international conference on open and big data (OBD) 2016 Aug 22 (pp. 25-30). IEEE.

[53] Zhou L, Wang L, Sun Y. MIStore: a blockchain-based medical insurance storage system. Journal of medical systems. 2018 Aug; 42(8):1-7.

[54] Al Omar A, Rahman MS, Basu A, Kiyomoto S. Medibchain: A blockchain based privacy preserving platform for healthcare data. InInternational conference on security, privacy and anonymity in computation, communication and storage 2017 Dec 12 (pp. 534-543). Springer, Cham.

[55] Zhang P, Schmidt DC, White J, Lenz G. Blockchain technology use cases in healthcare. In Advances in computers 2018 Jan 1 (Vol. 111, pp. 1-41). Elsevier.

[56] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In 2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[57] Maurya PK, Bagchi S. A secure PUF-based unilateral authentication scheme for RFID system. Wireless Personal Communications. 2018 Nov; 103(2):1699-712.

[58] Xu H, Ding J, Li P, Zhu F, Wang R. A lightweight RFID mutual authentication protocol based on physical unclonable function. Sensors. 2018 Mar 2; 18(3):760.

[59] Bendavid Y, Bagheri N, Safkhani M, Rostampour S. Iot device security: Challenging "a lightweight rfid mutual authentication protocol based on physical unclonable function". Sensors. 2018 Dec 15; 18(12):4444.

[60] Gope P, Lee J, Quek TQ. Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions. IEEE Transactions on Information Forensics and Security. 2018 May 3; 13(11):2831-43.

[61] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In 2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[62] Liang W, Xiao L, Zhang K, Tang M, He D, Li KC. Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems. IEEE Internet of Things Journal. 2021 Jan 22; 1-11.

[63] Farash MS, Nawaz O, Mahmood K, Chaudhry SA, Khan MK. A provably secure RFID authentication protocol based on elliptic curve for healthcare environments. Journal of medical systems. 2016 Jul; 40(7):1-7.

[64] Zhang L, Zhu S, Tang S. Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme. IEEE Journal of Biomedical and health informatics. 2016 Jan 12; 21(2):465-75.

[65] Siddiqui Z, Abdullah AH, Khan MK, Alghamdi AS. Smart environment as a service: three factor cloud based user authentication for telecare medical information system. Journal of medical systems. 2014 Jan; 38(1):1-4.

[66] Nyangaresi VO, Moundounga AR. Secure Data Exchange Scheme for Smart Grids. In 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[67] Madhusudhan R, Nayak CS. A robust authentication scheme for telecare medical information systems. Multimedia Tools and Applications. 2019 Jun; 78(11):15255-73.

[68] Dharminder D, Gupta P. Security analysis and application of Chebyshev Chaotic map in the authentication protocols. International Journal of Computers and Applications. 2021 Nov 26; 43(10):1095-103.

[69] Sureshkumar V, Amin R, Obaidat MS, Karthikeyan I. An enhanced mutual authentication and key establishment protocol for TMIS using chaotic map. Journal of Information Security and Applications. 2020 Aug 1; 53:102539.

[70] Xu X, Zhu P, Wen Q, Jin Z, Zhang H, He L. A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. Journal of medical systems. 2014 Jan; 38(1):1-7.

[71] Nyangaresi VO, Morsy MA. Towards Privacy Preservation in Internet of Drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[72] Guo C, Chang CC. Chaotic maps-based password-authenticated key agreement using smart cards. Communications in Nonlinear Science and Numerical Simulation. 2013 Jun 1; 18(6):1433-40.

[73] Hao X, Wang J, Yang Q, Yan X, Li P. A chaotic map-based authentication scheme for telecare medicine information systems. J Med Syst. 2013 Jun; 37(2): 1–7.

[74] Jiang Q, Ma J, Lu X, Tian Y. Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems. Journal of medical systems. 2014 Feb; 38(2):1-8.

[75] Amin R, Biswas GP. A secure three-factor user authentication and key agreement protocol for tmis with user anonymity. Journal of medical systems. 2015 Aug; 39(8):1-9.

[76] Wazid M, Das AK, Kumari S, Li X, Wu F. Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS. Security and Communication Networks. 2016 Sep 10; 9(13):1983-2001.

[77] Wang X, Fan K, Yang K, Cheng X, Dong Q, Li H, Yang Y. A new RFID ultra-lightweight authentication protocol for medical privacy protection in smart living. Computer Communications. 2022 Mar 15; 186:121-32.

[78] Nyangaresi VO, Abd-Elnaby M, Eid MM, Nabih Zaki Rashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 May 6, e4528: 1-16.

[79] Amir Latif RM, Hussain K, Jhanjhi NZ, Nayyar A, Rizwan O. A remix IDE: smart contract-based framework for the healthcare sector by using Blockchain technology. Multimedia tools and applications. 2020 Nov 10:1-24.

[80] Dharminder D, Mishra D, Li X. Construction of RSA-based authentication scheme in authorized access to healthcare services. Journal of medical systems. 2020 Jan; 44(1):1-9.

[81] Li CT, Shih DH, Wang CC. Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. Computer methods and programs in biomedicine. 2018 Apr 1; 157:191-203.

[82] Li CT, Lee CC, Weng CY, Chen SJ. A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems. Journal of medical systems. 2016 Nov; 40(11):1-0.

[83] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[84] Angelis J, Da Silva ER. Blockchain adoption: A value driver perspective. Business Horizons. 2019 May 1; 62(3):307-14.

[85] Tewari A, Gupta BB. An internet-of-things-based security scheme for healthcare environment for robust location privacy. International Journal of Computational Science and Engineering. 2020; 21(2):298-303.

[86] Li CT, Weng CY, Lee CC. A secure RFID tag authentication protocol with privacy preserving in telecare medicine information system. Journal of medical systems. 2015 Aug; 39(8):1-8.

[87] Zhou Z, Wang P, Li Z. A quadratic residue-based RFID authentication protocol with enhanced security for TMIS. Journal of ambient intelligence and humanized computing. 2019 Sep; 10(9):3603-15.

[88] Jiang Q, Chen Z, Li B, Shen J, Yang L, Ma J. Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems. Journal of Ambient Intelligence and Humanized Computing. 2018 Aug; 9(4):1061-73.

[89] Wu F, Xu L, Kumari S, Li X, Das AK, Shen J. A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications. Journal of Ambient Intelligence and Humanized Computing. 2018 Aug; 9(4):919-30.

[90] Radhakrishnan N, Karuppiah M. An efficient and secure remote user mutual authentication scheme using smart cards for Telecare medical information systems. Informatics in Medicine Unlocked. 2019 Jan 1; 16: 1-38.

[91] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV Computing-Assisted Search and Rescue Mission Framework for Disaster and Harsh Environment Mitigation. Drones. 2022 Jun 22; 6(7): 1-21.

[92] Chander B, Gopalakrishnan K. A secured and lightweight RFID-tag based authentication protocol with privacy-preserving in Telecare medicine information system. Computer Communications. 2022 May 13; 191: 425-437.

[93] Zheng L, Song C, Cao N, Li Z, Zhou W, Chen J, Meng L. A new mutual authentication protocol in mobile RFID for smart campus. IEEE Access. 2018 Oct 15; 6:60996-1005.

[94] Safkhani M, Vasilakos A. A new secure authentication protocol for telecare medicine information system and smart campus. IEEE Access. 2019 Feb 7; 7:23514-26.

[95] Salem FM, Amin R. A privacy-preserving RFID authentication protocol based on El-Gamal cryptosystem for secure TMIS. Information sciences. 2020 Jul 1; 527:382-93.

[96] Nyakomitta, P. S., Nyangaresi, V. O., & Ogara, S. O. Efficient Authentication Algorithm for Secure Remote Access in Wireless Sensor Networks. Journal of Computer Science Research. 2021 Aug; 3(4): 43-50.

[97] Islam SK, Khan MK. Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems. Journal of medical systems. 2014 Oct; 38(10):1-6..

[98] Jian G, Feng R. Cryptanalysis and improvement of an improved two factor authentication scheme for telecare medicine information systems. arXiv preprint arXiv:1607.01471. 2016 Jul 6.

[99] Li P, Nelson SD, Malin BA, Chen Y. DMMS: A decentralized blockchain ledger for the management of medication histories. Blockchain in healthcare today. 2019 Jun; 2: 1-22.

[100] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. In The Fifth International Conference on Safety and Security with IoT 2023 (pp. 81-99). Springer, Cham.

[101] Ravanbakhsh N, Nazari M. An efficient improvement remote user mutual authentication and session key agreement scheme for e-health care systems. Multimedia Tools and Applications. 2018 Jan; 77(1):55-88.

[102] Ostad-Sharif A, Abbasinezhad-Mood D, Nikooghadam M. An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC. International journal of communication systems. 2019 Mar 25; 32(5): 1-23.

[103] Qiu S, Xu G, Ahmad H, Wang L. A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems. IEEE access. 2017 Dec 8; 6:7452-63..

[104] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014; 16(5):137-44.

[105] Kumari S, Renuka K. Design of a password authentication and key agreement scheme to access e-healthcare services. Wireless Personal Communications. 2021 Mar; 117(1):27-45.

[106] Shamshad S, Ayub MF, Mahmood K, Rana M, Shafiq A, Rodrigues JJ. An identity-based authentication protocol for the telecare medical information system (TMIS) using a physically unclonable function. IEEE Systems Journal. 2021 Dec 2: 1-8.

[107] Fan K, Jiang W, Li H, Yang Y. Lightweight RFID protocol for medical privacy protection in IoT. IEEE Transactions on Industrial Informatics. 2018 Jan 18;14(4):1656-65.

[108] Barman S, Shum HP, Chattopadhyay S, Samanta D. A secure authentication protocol for multi-server-based e-healthcare using a fuzzy commitment scheme. IEEE Access. 2019 Jan 21; 7:12557-74.

[109] Ali Z, Hussain S, Rehman RH, Munshi A, Liaqat M, Kumar N, Chaudhry SA. ITSSAKA-MS: An improved three-factor symmetric-key based secure AKA scheme for multi-server environments. IEEE Access. 2020 Jun 10; 8:107993-8003.

[110] Nyangaresi V.O. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. In the 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612).

[111] Nikooghadam M, Amintoosi H. An improved secure authentication and key agreement scheme for healthcare applications. In 2020 25th International Computer Conference, Computer Society of Iran (CSICC) 2020 Jan 1 (pp. 1-7). IEEE.

[112] Limbasiya T, Sahay SK, Sridharan B. Privacy-preserving mutual authentication and key agreement scheme for multi-server healthcare system. Information Systems Frontiers. 2021 Aug; 23(4):835-48.