International Journal Of Latest Technology In Engineering & Management (IJLTEM)
Volume 8 - Issue 6 {November-December 2023} {Page: 42-50}

CYBER SECURITY IN HEALTHCARE SYSTEM: A SYSTEMATIC APPROACH OF MODERN THREADSAND DEVELOPMENT

M. Husain Bathushaw[1], Dr. S. Nagasundaram[2]
[1]*Research Scholar, VELS institute of science, technology and advanced studies, Pallavaram-600117, Chennai, India*
[2]*Research Supervisor/Asst. Professor, VELS institute of science, technology and advanced studies, Pallavaram-600117, Chennai, India*

Abstract: *This study explores the vital area of cyber security in healthcare systems, focusing on emerging risks as well as technological developments. Using a descriptive methodology and secondary data collecting, the study takes a logical approach and interpretivist philosophy. Based on the investigation, a dynamic threat environment with sophisticated assaults which includes phishing, ransom ware, and supply chain vulnerabilities is discovered. Although the security procedures in place have been strengthened by legislative frameworks that include GDPR and HIPAA, there are still loopholes. To strengthen cyber security, the suggested framework combines multi-factor authentication, and enhanced threat detection, including extensive training initiatives. Implementation and resource allocation issues continue to be present, though. Suggestions include customized approaches, cooperative alliances, and continuous risk evaluations. Subsequent investigations have chosen to focus on nascent technology, the consequences of regulations, extended danger assessment, and human aspects. This research proposes a thorough framework for improving cyber security in the healthcare industry, protecting patient information, includingguaranteeing continuous healthcare services.*

Keywords: *Healthcare, Cyber security, Threat Landscape, Regulatory Frameworks, Advanced Technologies.*

INTRODUCTION

A. Research Background

Electronic health records, telemedicine, including networked medical equipment are becoming essential parts of contemporary healthcare delivery, indicating a significant digital revolution in the healthcare industry. However as the industry becomes more dependent on technology, a wide range of cyber threats are becoming more prevalent [1]. A successful cyber attack on the healthcare industry could result in disastrous repercussions, compromising patient data or causing interruptions to essential medical services. Strong cyber security measures are urgently needed, as demonstrated by the rise in cyber-attacks that have targeted healthcare organizations in recent years. Healthcare data security is governed by tight regulations, including the Health Insurance Portability and Accountability Act (HIPAA), which places strong requirements on protecting patient data [2]. The dynamic and comprehensive approach to cyber security needs to be taken due to the ever-evolving nature of cyber threats, even with these regulatory actions in place. This study attempts to give a methodical investigation of the current cyber threats that healthcare systems face, assessing their consequences as well as putting forward creative solutions to strengthen the industry's digital defenses. The project intends to make a contribution to the security and resilience of healthcare infrastructures in a world that is becoming more linked by filling up this important knowledge gap.

B. Aims and Objectives

Aims

The primary aim of this research is to improve healthcare systems' cyber security posture by methodically comprehending contemporary dangers as well as advancements.

Objectives:

- To perform a thorough assessment as well as evaluation of the literature on cyber security in healthcare systems, including historical views and contemporary trends.

- To classify and evaluate current cyber attacks that have targeted healthcare organizations, discovering common attack vectors, causes, as well as consequences.
- To assess critically the effectiveness of current regulatory frameworks—like HIPAA—in combating modern cyber threatsand to recommend possible revisions or additional actions.
- To create a thorough cyber security architecture that includes proactive risk management techniques, enhanced threat detection, as well as incident response procedures that are specifically adapted to the requirements and difficulties faced by healthcare institutions.

C. Rationale

While the digitalization of healthcare systems has revolutionized patient care, it also renders the industry more vulnerable to growing cyber threats. These risks, which include everything from ransom ware attacks to data breaches, seriously jeopardize patient privacy as well as the continuous provision of essential healthcare services [3]. A systematic strategy is of the utmost importance to fully comprehend and reduce these dangers, according to current literature. Furthermore, because cyber dangers are always changing, research must be done continuously in order to stay ahead of new strategies. The purpose of this study is to close this crucial gap by methodically analyzing contemporary cyber threats in the healthcare industry and creating specialized tactics to strengthenthe industry's digital defenses and protect patient welfare.

LITERATURE REVIEW

A. Historical Perspectives on Cyber security in Healthcare

Numerous notable achievements and difficulties have accompanied the development of cybersecurity in the healthcare industry. Healthcare systems gave little thought to appropriate security measures in the early phases of digitalization and were instead focused on automating administrative procedures. As a result, there were weaknesses that were taken advantage of as hackers found the healthcare industry to be a lucrative target [6]. Healthcare data breaches spiked in the early 2000s, leading to US governmental remedies including the Health Insurance Portability and Accountability Act (HIPAA) [4]. HIPAA implemented harsh fines for non-compliance while establishing strict guidelines for protecting patient data. The attack surface was significantly increased in the years that followed with the increasing use of linked medical devices including the expansion of electronic health records (EHRs) [5]. Sophisticated cyber threats, which include ransom ware assaults and deliberate phishing efforts, increased as a result. Gaining an appreciation of this historical background is essential for comprehension of the present status of cyber security in the healthcare industry. It also underlines the need for constant innovation and adaptation to protect sensitive patient data andessential healthcare services.

B. Emerging Trends in Cyber Threats Targeting Healthcare Systems

The healthcare industry has seen an increase in sophisticated cyberthreats in recent years, which is indicative of a dynamic environment with constantly changing attack vectors. These days, ransomware attacks are a major concern since hackers are using more sophisticated methods to encrypt important patient data and then demand large ransoms to unlock the keys [11]. Furthermore, sophisticated targeted phishing attempts have begun to employ social engineering techniques to obtain unauthorized access to private healthcare networks. The exploitation of vulnerabilities in third-party vendors including service providers by adversaries to obtain unauthorized access to healthcare systems is a disturbing trend known as supply chain assaults [12]. Moreover, the spread of Internet of Things (IoT) devices in healthcare environments has opened up new opportunities for abuse because these gadgets do not have strong security safeguards. Furthermore, the dark web market for pilfered medical records has grown and is becoming a profitable sector for online thieves. This tendency calls for more caution when it comes to patient data security.

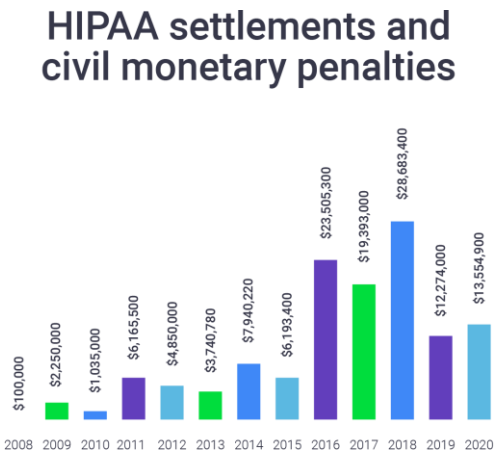

Figure 1: Emerging Trends in Cyber Threats Targeting Healthcare Systems

C. Regulatory Frameworks and Compliance Standards for Healthcare Data Security

Patient information privacy in the healthcare sector is tightly controlled by a complex regulatory framework. The Health Insurance Portability and Accountability Act (HIPAA) in the US is one of the key foundations.
Comprehensive security measures are required by HIPAA in order to guarantee the privacy, availability, and integrity of electronic protected health information (ePHI) [7]. It is necessary for covered companies including their business partners to put in place technological, administrative, in addition to physical safeguards to protect patient data. Comparably, the European Union's General Data Protection Regulation (GDPR) lays forth strict guidelines for data protection, with especially close attention to healthcare data [8]. It gives people rights over their personal data, enforces stringent breach notification deadlines, and requires express consent for data processing. Other international standards, which include NIST SP 800-53 and ISO/IEC 27001, offer frameworks for information security management systems that are widely accepted and could possibly be used by healthcare organizations looking to set up thorough security procedures. Healthcare organizations must abide by these regulatory frameworks in order to protect patient privacy and security, as well as to minimize the financial and legal ramifications of non-compliance.

Figure 2: Regulatory Frameworks and Compliance Standards for Healthcare Data Security

D. Effectiveness of Existing Measures in Mitigating Cyber Risks in Healthcare

Healthcare cybersecurity strategies now in use have positive and negative effects. Unquestionably, regulatory frameworks like HIPAA have been crucial in promoting awareness as well as establishing minimum security procedures. They have compelled healthcare institutions to put policies in place including encryption, frequent security audits, and access limitations [9]. Nevertheless, a dynamic strategy is required due to the ever-evolving nature of cyber threats. HIPAA offers a strong foundation, but new attack vectors could fail to be able to keep up with it. The necessity for more proactive measures, which include strong backup and recovery procedures and extensive staff training programs to thwart phishing assaults, has been highlighted by emerging threats like ransomware [10]. Moreover, a more comprehensive ecosystem approach—which involves safe supply chain management including cooperation with outside vendors—is necessary due to the interconnectedness of

healthcare systems.

E. Literature Gap

The majority of the material currently available on cyber security in healthcare is devoted to regulatory compliance, and historical views, including threat assessments [13]. Research that methodically tackles the dynamic nature of new cyber threats in addition to suggesting creative, situation-specific methods for strengthening healthcare systems against these changing threats is conspicuously lacking, nevertheless. The goal of this investigation is to closethis important information gap.

METHODOLOGY

The interpretivist theory used in this study acknowledges the subjectivity of cybersecurity practices and perceptions in healthcare settings. Interpretivism emphasizes the important role of comprehending stakeholders' viewpoints and the numerous contextual elements driving cybersecurity choices, which is in line with the complex as well as the socially constructed character of cybersecurity. We'll use a logical technique to test theories based on accepted cybersecurity concepts against actual healthcare situations [14]. This technique providesempirical insights into the efficacy of cybersecurity solutions by enabling systematic testing as well as validation of theoretical frameworks in real-world scenarios. In order to give a thorough perspective of the cybersecurity environment in healthcare, a descriptive research design is used. This architecture makes it less difficult to gather comprehensive, contextual data on current procedures, perceived threats, and the application of security measures [15]. The study uses secondary data that was gathered from reliable sources, such as databases of cybersecurity incidents, industry reports, and government publications, including scholarly journals. This strategy involves the use of the body of current information to generate a thorough grasp of the advancements in healthcare systems as well as contemporary cybersecurity threats. The chosen articles and publications for examination are current as of 2010 or later to guarantee their applicability to current cybersecurity issues. Furthermore, sources from reputable authorities in cybersecurity together with healthcare fields are given precedence [16]. Relevant data, such as attack paths, impactevaluations, kinds of cyber threats, and current security measures, are extracted in a methodical manner. After that, this data is combined in order to identify recurrent themes and new trends. The gathered material is put through a thematic analysis, which classifies it into important topics like ransomware, phishing, and other types of cyberthreats; vulnerabilities, including unpatched software and insider threats; and current countermeasures, with the value firewalls and encryption techniques. On the basis of well-established cybersecurity concepts, derived hypotheses are applied to the combined data. The goal of this procedure is to either enhance or validate current theoretical frameworks in relation to cybersecurity in healthcare. Results are cross-verified against several sources as well as validated using actual case studies of noteworthy cyber events in the healthcare industry to guarantee the validity of the conclusions. Using this technological technique, the research seeks to give a thorough and independently confirmed overview of current cybersecurity risks in the healthcare industry, providing important information for the creation of successful securityplans in this vital field.

RESULTS

A. Analysis of Modern Cyber Threats in Healthcare Systems

The examination of contemporary cyber threats in healthcare systems reveals a complex environment with dynamic attack pathways including advanced strategies. Attackers using sophisticated encryption methods to lock down vital patient data are known to employ ransomware as a common threat, and they frequently demand astronomical ransoms in exchange for the decryption keys. Critical healthcare services have been disrupted as a consequence of these attacks, endangering patient safety [17]. Healthcare workers are the subject of increasingly complex phishing attempts that make use of social engineering techniques to obtain unauthorized access to private networks. These efforts are difficult to identify because they frequently use phony emails or statements that seem authentic. Concern over supply chain assaults is rising as attackers penetrate healthcare systems by using advantage of weaknesses in third-party suppliers and service providers. This pattern emphasizes how important it is to thoroughly screen and keep an eye on outside collaborators inside the healthcare system [18].

Moreover, the spread of Internet of Things (IoT) devices in healthcare environments creates new opportunities for abuse. Although these gadgets improve medical care including monitoring, they do not have strong security safeguards, which might allow cyber attackers to access them. The report emphasizes how evolving and adaptable cyber threats are in the healthcare industry. It highlights the significance it is to having a proactive, multi-layered cybersecurity approach in order to successfully reduce these threats. This entails frequent vulnerability assessments, strong access restrictions, and staff training initiatives, including ongoing monitoring [19]. Furthermore, the results emphasize the necessity of cooperative endeavors between healthcare establishments, regulatory agencies, as well as technology providers to strengthen the industry's digital safeguards against a constantly changing arrayof threats.

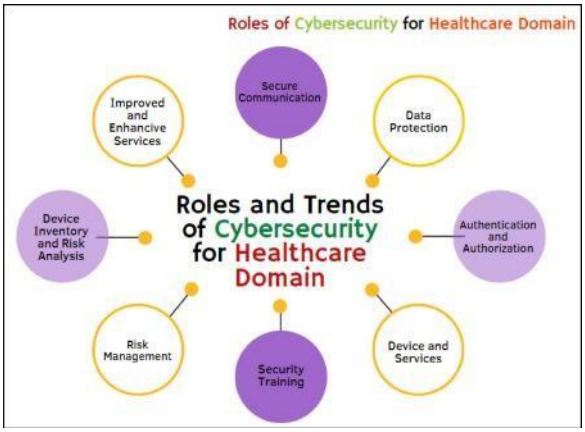

Figure 3: Cyber security in healthcare Domain

B. Effectiveness of Existing Cyber security Measures Healthcare Systems

Current cyber security safeguards are evaluated, and the results show both their benefits as well as their drawbacks Laws which includeHIPAA have certainly strengthened securityprocedures by requiring extensive protections for electronically protected health information (ePHI). These precautions consist of encryption guidelines, access controls, and recurring security audits. However the changing nature of cyber threats necessitates a more flexible strategy [20]. HIPAA compliance offers a strong foundation, but it could occasionally not be able to keep up with the speed at which attack vectors are developing. To successfully prevent phishing attempts, for example, new and emerging dangers which include ransom ware have shown the necessity for more proactive measures, including solid backup and recovery policies combined with extensive employee training programs [21]. In addition, the requirement for safe supply chain management is expanding as healthcare systems become more integrated. It is of the utmost importance to exercise caution while evaluating and keeping an eye on outside suppliers and service providers in order to stop possible weaknesses from being takenadvantage of. The ongoing adoption and integration ofcutting-edge technology are also essential to theefficacy of current policies [22]. This involvesintegrating artificial intelligence for anomaly detection, putting in place real-time monitoring tools, including deploying sophisticated threat detection systems. In conclusion, while the security posture of healthcare organizations has unquestionably beenreinforced by current efforts, a dynamic andmultifaceted strategy is required to stay ahead of thealways changing cyber threat scenario. To guarantee the continuous safety of sensitive patient information and the continuous provision of essential healthcare services, this calls for a mix of technology improvements, regulatory compliance, as well asextensive training and awareness campaigns.

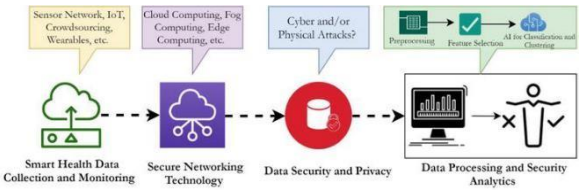

Figure 4: Smart Health and Cyber security in the Era of Artificial Intelligence

C. Compliance with Regulatory Frameworks and Standards

Healthcare companies have advanced a long way in complying with regulations and laws intended to protect patient information. A keystone in this effort is the Health Insurance Portability and Accountability Act (HIPAA), a law that demands stringent safeguards for electronic protected health information (ePHI) [23]. To guarantee compliance, covered companies including their business partners have put in place strong administrative, physical, as well as technical measures. Furthermore, healthcare organizations throughout the globe have been compelled to improve their data privacy protocols by the General Data Privacy Regulation (GDPR) in the European Union [24]. Globally, there has been a movement towards more thorough data protection practices due to GDPR's emphasis on transparent data processing, strict breach notification timescales, and the provisionof individuals control over their personal data.Internationally accepted frameworks like as NIST SP 800-53 and ISO/IEC 27001 have also become more widely recognized [25]. These standards give a methodical approach to the application of cybersecurity by providing organized rules for the creation as well as upkeep of information security management systems. Despite the fact that compliance initiatives have improved data security, problems still exist. Certain organizations could have encountered resource limitations while attempting to completely implement complicated safeguards, which might leave them open to developing threats. Furthermore, because cyber hazards are dynamic, it's essential to bevigilant and adjust to new threats.

Data Protection Regulation)	processing, strict breach notification timelines, and individual data rights	comprehensive data protection practices.
ISO/IEC27001	Information security management system establishment and maintenance	Provided a structured approach to cybersecurity implementation.
NIST SP 800-53	Guidelines for establishing information security controls	Offered systematic guidance for managing information security.

D. Proposed Framework for Enhanced Cybersecurityin Healthcare

Depending on the examination of contemporary cyber threats and the appraisal of current countermeasures, a thorough framework has been recommended to strengthen healthcare systems' cybersecurity posture. This framework aims to offer a strong defense against changing threats by integrating best practices and technology breakthroughs.

Regulatory Framework	**Key Emphasis**	**Impact on Healthcare Security**
HIPAA	Protection of ePHI, administrative, physical, technical safeguards	Strengthened data protection and access control measures.
GDPR (General	Transparent data	Encouraged the global adoption of

Advanced Threat Detection and Response Systems: Using state-of-the-art technology, such as machinelearning and artificial intelligence, to react in a timely manner to any attacks in real time while continually monitoring network traffic and identifying anomalies [26].

Multi-factor authentication, or MFA, is a security measure that goes beyond simple passwords and usernames by requiring the usage of MFA for allsystem access. This guarantees that sensitive data canonly be accessed by authorized persons.

Regular Security Training and Awareness Programs: Putting in place regular, specialized training to help healthcare workers spot and handle social engineering scams, phishing scams, and additional possible security lapses.

Endpoint security as well as device management: Using strong endpoint security solutions to protect against malware while additionally making sure that all network-connected devices adhere to strict securityguidelines.

Data Encryption and Secure Communication Protocols: To prevent unwanted access or interception, important patient information should be encrypted end-to-end while it's in transit and at rest.

CRITICAL EVALUATION ANDRECOMMENDATIONS

A. Critical Evaluation

It is admirable that a framework for improved cybersecurity in the healthcare industry has been presented in order to cope with the intricate and constantly changing threat landscape that the industry faces. A forward-thinking strategy is demonstrated bythe integration of robust endpoint security, multi- factor authentication, as well as sophisticated threat detection technologies. These steps might greatly improve the security posture of healthcare organizations and are in line with industry best practices. Notwithstanding, obstacles could emerge during the pragmatic use of this structure. While encouraging, integrating cutting-edge technology necessitates a significant financial commitment and a high level of technical proficiency [27]. It can bedifficult for smaller medical facilities with fewer resources to cultivate widespread acceptance. Furthermore, depending on the size and structure of the organization, different training programs and cultural changes towards a security-conscious attitudecould fail to be as successful [28]. While ongoing evaluation and surveillance of compliance is crucial, it can be logistically difficult to provide resources and expertise. Furthermore, because cyber dangers are always changing, a dynamic structure that is capable of adapting to new threats is required.

B. Recommendations

Tailored Implementation Plans: Tailor the suggested cybersecurity framework according to every healthcare organization's unique requirements as well as available resources. Give instructions for a gradual deployment

that takes into consideration the workforce's capabilities, the infrastructure that is already in place, and budgetary restrictions.

Training and Allocation of Resources: Provide enough funds for hiring new employees, and training them, including continuing upkeep of the equipment [29]. Provide training courses that meet the varying skill levels of employees in the company to guaranteethat they are all prepared to handle cyberattacks.

Collaboration Agreements: Promote cooperation between government agencies, technological companies, and healthcare organizations. Encourage the development of best practice forums and information-sharing networks in order to encourage group learning and fortify the cybersecurity ecosystem as a whole.

Regular Risk Assessments and Updates: To find new threats and weaknesses, conduct risk assessments on a regular basis. For sure that the cybersecurity framework remains relevant and effective, it needs to be updated to include new technology and best practices.

Drills for Incident Response: Plan frequent incident response exercises to evaluate the effectiveness of the established protocols. This will guarantee that employees are aware of their responsibilities in the event of a cyber incident and assist in identifying areasfor improvement.

Third-Party Vendor Investigation: Boost third-party suppliers' and service providers' due diligence processes. Put in place stringent hiring procedures and precisely define contractual duties in relation to cybersecurity practices.

C. Future Work

Future studies in cybersecurity in healthcare should concentrate on a number of important issues. First, investigating what happens when to better detect threats and secure data by integrating cutting-edge technology like blockchain and artificial intelligence. It is also crucial to look at the manner in which changing regulatory frameworks affect future cyber hazards and the way well they function to mitigate them. Additionally, longitudinal research monitoring the development of cyber threats and the adjustment of security protocols inside healthcare institutions will yield important insights [30]. Finally, studying user behavior and organizational culture in relation to cybersecurity will be essential for creating awareness-raising and training initiatives that are specifically aimed at this population. These research directions will help create a healthcare cybersecurity environment that is more adaptable and robust.

REFERENCE

[1] *Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E. and Bonacina, S., 2021. Influence of humanfactors on cyber security within healthcare organisations: A systematic review. Sensors, 21(15), p.5119.*

[2] *National Academies of Sciences, Engineering, and Medicine, 2019. Taking action against clinician burnout: a systems approach to professional well-being.*

[3] *Marques, G., Pitarma, R., M. Garcia, N. and Pombo, N., 2019. Internet of things architectures, technologies, applications, challenges, and future directions for enhanced living environments and healthcare systems: a review. Electronics, 8(10), p.1081.*

[4] *Ahmad, K.A.B., Khujamatov, H., Akhmedov, N., Bajuri, M.Y., Ahmad, M.N. and Ahmadian, A., 2022. Emerging trends and evolutions for Smart city healthcare systems. Sustainable Cities andSociety, 80, p.103695.*

[5] *Geršak, J., 2022. Design of Clothing Manufacturing Processes:A Systematic Approach to Developing, Planning, and Control. Woodhead Publishing.*

[6] *Sworna, N.S., Islam, A.M., Shatabda, S. and Islam, S., 2021. Towards development of IoT-ML driven healthcare systems: A survey. Journal of Network and Computer Applications, 196, p.103244.*

[7] *Ross, R., Pillitteri, V., Graubart, R., Bodeau, D. and McQuaid, R., 2019. Developing cyber resilient systems: a systems security engineering approach (No. NIST Special Publication (SP) 800-160 Vol. 2 (Draft)). National Institute of Standards and Technology.*

[8] *Pang, T.Y., Pelaez Restrepo, J.D., Cheng, C.T., Yasin, A., Lim, H. and Miletic, M., 2021. Developing a digital twin and digital thread framework for an 'Industry 4.0'Shipyard. Applied Sciences, 11(3), p.1097.*

[9] *Alfaqiri, A., Hossain, N.U.I., Jaradat, R., Abutabenjeh, S., Keating, C.B., Khasawneh, M.T. and Pinto, C.A., 2019. A systemic approach for disruption risk assessment in oil and gas supply chains. International Journal of Critical Infrastructures, 15(3), pp.230-259.*

[10] *Kumar, P.M., Lokesh, S., Varatharajan, R., Babu, G.C. and Parthasarathy, P., 2018. Cloud and IoT based disease prediction anddiagnosis system for healthcare using Fuzzy neural classifier. Future Generation Computer Systems, 86, pp.527-534.*

[11] *Nazah, S., Huda, S., Abawajy, J. and Hassan, M.M., 2020. Evolution of dark web threat analysis and detection: A systematic approach. Ieee Access, 8, pp.171796-171819.*

[12] *Shafqat, S., Kishwer, S., Rasool, R.U., Qadir, J., Amjad, T. and Ahmad, H.F., 2020. Big data analytics enhanced healthcare systems:a review. The Journal of Supercomputing, 76, pp.1754-1799.*

[13] *Camp, L.J., Grobler, M., Jang-Jaccard, J., Probst, C., Renaud, K. and Watters, P., 2019. Measuring human resilience in the face ofthe global epidemiology of cyber attacks.*

[14] *Mosqueira-Rey, E., Alonso-Ríos, D., Moret-Bonillo, V., Fernández-Varela, I. and Álvarez-Estévez, D., 2018. A systematic approach to API usability: Taxonomy-derived criteria and a case study. Information and Software Technology, 97, pp.46-63.*

[15] *Mujawar, M.A., Gohel, H., Bhardwaj, S.K., Srinivasan, S., Hickman, N. and Kaushik, A., 2020. Nano-enabled biosensing systems for intelligent healthcare: towards COVID-19 management.Materials Today Chemistry, 17, p.100306.*

[16] *Kumar, A., Singh, A.K., Ahmad, I., Kumar Singh, P., Anushree, Verma, P.K., Alissa, K.A., Bajaj, M., Ur Rehman, A. and Tag-Eldin, E., 2022. A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacksin healthcare. Sensors, 22(15), p.5921.*

[17] *Gardašević, G., Katzis, K., Bajić, D. and Berbakov, L., 2020. Emerging wireless sensor networks and Internet of Things technologies—Foundations of smart healthcare. Sensors, 20(13), p.3619.*

[18] *Dey, N., Ashour, A.S., Shi, F., Fong, S.J. and Tavares, J.M.R., 2018. Medical cyber-physical systems: A survey. Journal of medical systems, 42, pp.1-13.*

[19] *Mangnus, E. and Van Westen, A.C.M., 2018. Roaming through the maze of maize in northern Ghana. A systems approach to explorethe long-term effects of a food security intervention. Sustainability,10(10), p.3605.*

[20] *Ignaczak, L., Goldschmidt, G., Costa, C.A.D. and Righi, R.D.R., 2021. Text mining in cybersecurity: A systematic literature review. ACM Computing Surveys (CSUR), 54(7), pp.1-36.*

[21] *Neyens, D.M., Bayramzadeh, S., Catchpole, K., Joseph, A., Taaffe, K., Jurewicz, K., Khoshkenar, A., San, D. and Group, R.O.S., 2019. Using a systems approach to evaluate a circulating nurse's work patterns and workflow disruptions. Applied ergonomics, 78, pp.293-300.*

[22] *Ghazal, T.M., Hasan, M.K., Alshurideh, M.T., Alzoubi, H.M.,Ahmad, M., Akbar, S.S., Al Kurdi, B. and Akour, I.A., 2021. IoT for smart cities: Machine learning approaches in smart healthcare—A review. Future Internet, 13(8), p.218.*

[23] *Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P. and Janicke, H., 2020. A holistic review of cybersecurity and reliabilityperspectives in smart airports. IEEE Access, 8, pp.209802-209834.*

[24] *Stallings, W., 2018. Effective cybersecurity: a guide to using best practices and standards. Addison-Wesley Professional.*

[25] *Verdejo Espinosa, Á., Lopez, J.L., Mata Mata, F. and Estevez, M.E., 2021. Application of IoT in healthcare: keys to implementation of the sustainable development goals. Sensors, 21(7), p.2330.*

[26] *Bhuiyan, M.N., Rahman, M.M., Billah, M.M. and Saha, D., 2021. Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. IEEE Internet of Things Journal, 8(13), pp.10474- 10498.*

[27] *Larriva-Novo, X., Vega-Barbas, M., Villagra, V.A., Rivera, D., Alvarez-Campana, M. and Berrocal, J., 2020. Efficient distributed preprocessing model for machine learning-based anomaly detectionover large-scale cybersecurity datasets. Applied Sciences, 10(10), p.3430.*

[28] *Azeez, N.A. and Van der Vyver, C., 2019. Security and privacyissues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal, 20(2), pp.97-108.*

[29] *Sallos, M.P., Garcia-Perez, A., Bedford, D. and Orlando, B., 2019. Strategy and organisational cybersecurity: a knowledge-problem perspective. Journal of Intellectual Capital, 20(4), pp.581-597.*

[30] *Martynov, V.V., Shavaleeva, D.N. and Zaytseva, A.A., 2019, September. Information technology as the basis for transformation into a digital society and industry 5.0. In 2019 International Conference" Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS) (pp. 539-543). IEEE.*