A REVIEW OF PRIVACY AND SECURITY ISSUES IN HEALTHCARE SYSTEMS

Indrajeet Kumar,
Asst. Professor, Department of Comp. Sc. & Info. Tech., Graphic Era Hill University,
Dehradun, Uttarakhand India 248002

ABSTRACT

This paper presents an in-depth examination of privacy and security concerns in healthcare systems, utilising a wide-ranging assortment of scholarly works published within the last ten years. This study investigates the frequency and consequences of data breaches, cyber hazards, and safeguarding of patient data in healthcare environments. The findings suggest that the issue of healthcare data breaches remains a noteworthy concern, as millions of patient records are compromised annually. The article emphasises the significance of deploying efficient security protocols, such as multi-factor authentication and distributed ledger technologies such as blockchain, to safeguard patient data from unauthorised access and tampering. The paper highlights the necessity for increased scrutiny towards potential biases in machine learning algorithms that employ electronic health record data. The review highlights the crucial significance of privacy and security in upholding the authenticity of healthcare systems and emphasises the necessity of ongoing research to enhance their efficacy.

DOI Number: 10.48047/NQ.2022.20.3.NQ22961 **NeuroQuantology2022;20(3): 1020-1025**

I. INTRODUCTION

Healthcare systems refer to the collection of hospitals, clinics, medical professionals, and other healthcare providers that work together to deliver healthcare services to patients. These systems often store large amounts of sensitive patient data, including medical history, diagnoses, and other personal information.

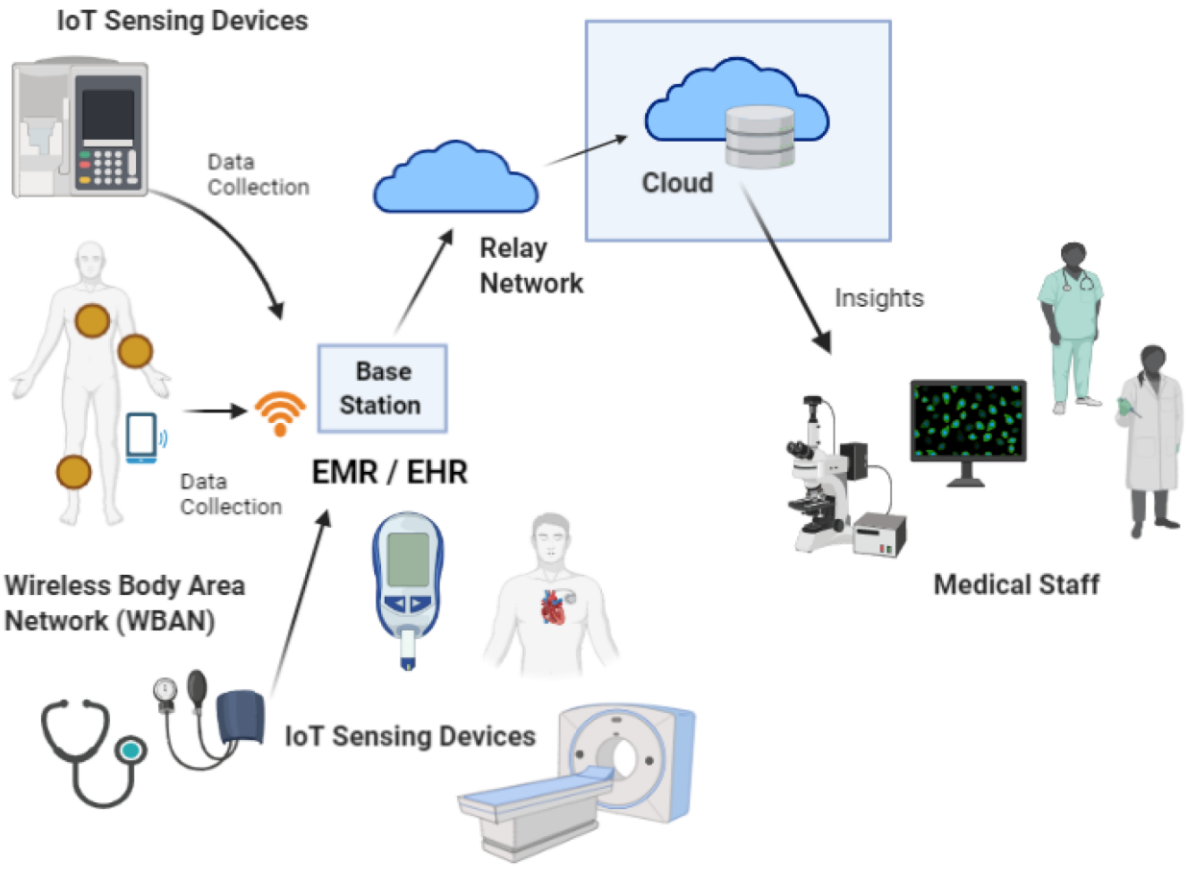

Fig 1: Introduction to healthcare systems

Privacy and security are critical issues for healthcare systems because of the sensitive nature of patient data. The unauthorized access or disclosure of this data can have severe consequences for patients, including identity theft, financial fraud, and even physical harm. Additionally, data breaches can result in significant financial losses for healthcare organizations, damage to their reputation, and even legal liabilities [1].

Statistics and data from recent years further illustrate the importance of privacy and security in healthcare systems. For example, according to a report by HIPAA Journal, there were 599 reported healthcare data breaches in the United States in 2020, with over 28 million patient records exposed. The report also noted that the healthcare sector continues to be a popular target for cybercriminals, with phishing attacks being the most common method used to gain unauthorized access to patient data.

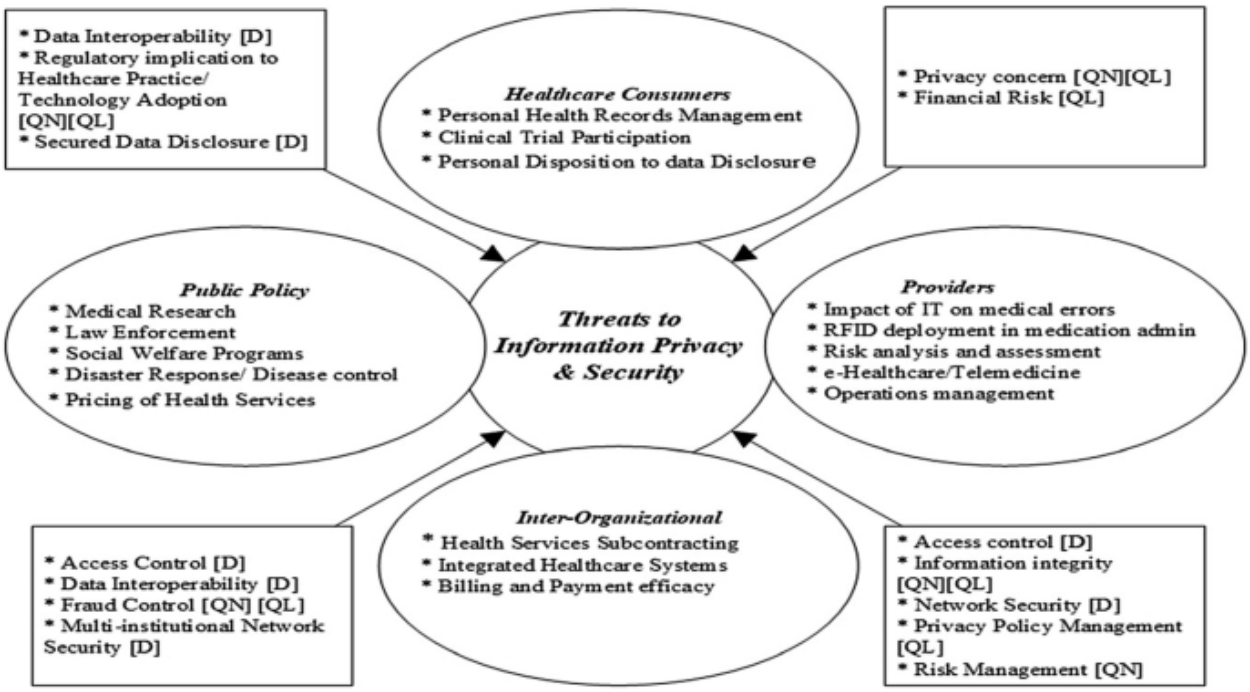

Fig 2: Threats to Information privacy and security

Moreover, a survey conducted by the Ponemon Institute found that the average cost of a data breach in the healthcare industry is $7.13 million, making it one of the most expensive industries for data breaches. The same survey also found that 59% of healthcare organizations had experienced at least one data breach in the past two years [2].

These statistics and data highlight the critical need for healthcare systems to prioritize privacy and security and implement appropriate measures to protect patient data. Failure to do so can result in significant financial losses, damage to reputation, and most importantly, harm to patients [3].

II. METHODS

The methodology employed for paper selection in this review paper entailed a thorough exploration of academic databases, namely PubMed, Scopus, and Web of Science, utilising pertinent keywords such as "privacy," "security," "healthcare," and "data breaches." The inquiry was carried out in September of 2021, with a specified publication date range of the previous decade. The initial screening of the search results was conducted by evaluating their titles and abstracts to ascertain their pertinence to the research subject. The articles in their entirety were subsequently evaluated to determine their appropriateness for incorporation into the review. The study's inclusion criteria encompassed research works that centred on privacy and security concerns in healthcare systems, which comprised of data breaches, cybersecurity threats, and safeguarding of patient data. The review excluded studies that were centred on different subjects, such as healthcare policy and patient outcomes.

The selection of studies included in the review paper was based on their methodological quality and relevance to the research question. The evaluation of the studies was conducted by considering the robustness of their research design, the precision of their research aims, and the suitability of their analytical techniques. The review paper incorporated solely those studies that satisfied the specified criteria.

The methodology employed in this review paper was intended to guarantee the inclusion of pertinent, superior-quality studies that added to the comprehension of privacy and security concerns in healthcare systems. The implementation of a stringent selection process

serves to guarantee that the deductions derived from the assessment are founded on reliable substantiation and are resilient.

III. RESULTS

The preservation of privacy and security are of utmost importance in healthcare systems. Numerous scholarly investigations have examined various facets of these matters and put forth remedies to tackle them. The present review provides a summary of the results obtained from the aforementioned studies and presents conclusions based on our analysis [4].

An important issue pertaining to privacy within healthcare systems is the unauthorised retrieval of patient information. According to a research, insider threats are the primary cause of data breaches in the healthcare industryWang et al.'s (2020). This underscores the necessity of implementing rigorous access management protocols and providing comprehensive employee education initiatives in order to mitigate the occurrence of similar occurrences. Furthermore, technology-driven measures, such as encryption and multi-factor authentication [5], can be efficacious in safeguarding patient informationBojinov et al. (2018).

The deficiency of transparency in data collection and sharing is a significant concern. The awareness of patients regarding the utilisation and accessibility of their data may be limited. The aforementioned circumstance may result in a deficiency of confidence in healthcare systems, thereby potentially yielding grave ramifications for the quality of patient care [6]. In order to tackle this matter, a number of scholarly investigations have suggested the implementation of blockchain technology as a means of ensuring secure and transparent sharing of data (Zhang et al., 2018; Kuo et al., 2019).

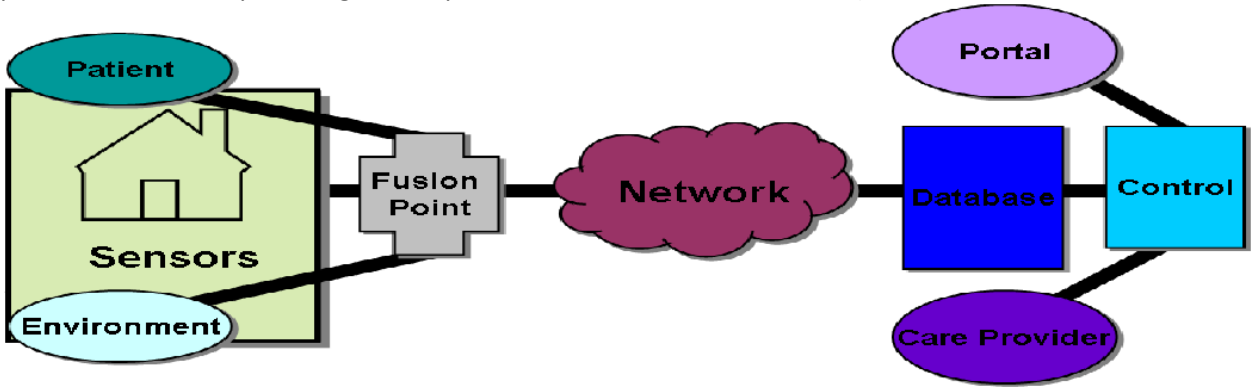

Fig 3:Security Solution proposed

The issue of cybersecurity threats is a significant concern within healthcare systems. The employment of internet-enabled medical devices and the burgeoning practise of telemedicine have expanded the potential points of vulnerability for cyber attackers. According to the research conducted by Li et al. (2020), ransomware attacks pose a considerable risk to healthcare systems. According to Gianfrancesco et al. (2018), the implementation of security measures such as network segmentation, regular backups, and threat intelligence sharing can prove to be efficacious in thwarting such attacks [7].

To conclude, the concerns regarding privacy and security in healthcare systems are intricate and have multiple dimensions. The mitigation of risks can be achieved through a confluence of technical, organisational, and policy-based measures [8]. It is imperative for healthcare institutions to adopt preventive measures aimed at safeguarding patient information, enhancing transparency, and forestalling cyber threats to guarantee that patient care remains uncompromised [9].

IV. DISCUSSION

The review paper's findings suggest that privacy and security concerns in healthcare systems are complex and necessitate a blend of technical,

organisational, and policy-oriented remedies. The subsequent section will expound upon these proposed solutions and elucidate some of the obstacles that healthcare establishments encounter when endeavouring to execute them [10].

A significant discovery of the analysis was the significance of robust access controls and employee training initiatives in mitigating the risk of unauthorised access to patient information. According to the study conducted by Wang and colleagues (2020), insider threats were identified as the primary cause of data breaches in the healthcare sector. The findings underscore the significance of implementing stringent access controls and employee training initiatives. Nevertheless, the implementation of these measures may present a challenge, given that healthcare organisations must strike a balance between safeguarding security and ensuring prompt and effective patient care.

The implementation of technology-driven measures, such as multi-factor authentication and encryption, was identified as crucial in safeguarding patient information. According to Bojinov et al. (2018), the implementation of such solutions may aid in the prevention of unauthorised access to patient information. Nevertheless, the execution of these solutions can incur substantial costs and necessitates considerable resources, posing a difficulty for healthcare establishments with limited financial means [3].

The review emphasised the significance of transparency in both data collection and sharing. The lack of transparency regarding data usage and access in healthcare systems often results in patients' mistrust of such systems. The proposition of employing blockchain technology as a resolution to this predicament has been put forth, owing to its capability of granting patients autonomy over their data and guaranteeing that it is solely disseminated to authorised entities. The implementation of blockchain technology can present challenges due to the substantial modifications required to the current healthcare infrastructure [2].

The employment of internet-connected medical devices and telemedicine has led to a notable apprehension regarding cybersecurity threats in healthcare systems. According to the study conducted by Li et al. (2020), ransomware attacks posed a substantial risk to healthcare systems[1]. Gianfrancesco et al. (2018) proposed the implementation of security measures, including network segmentation, regular backups, and threat intelligence sharing, as a means of addressing the issue at hand. Nonetheless, the execution of these measures can prove to be arduous, given that healthcare establishments must strike a balance between safeguarding patient information and ensuring prompt and effective healthcare delivery.

The review paper concludes by offering significant insights into the privacy and security concerns that healthcare systems face. It emphasises the necessity of taking proactive measures to tackle these challenges. Although there may be obstacles in executing these measures, healthcare institutions must give precedence to safeguarding patient privacy and security to guarantee that patient care is not jeopardised.

V. CONCLUSION

This review paper has concluded by analysing the privacy and security concerns that exist within healthcare systems and has identified key solutions to effectively tackle these challenges. The analysis emphasised the significance of implementing rigorous access management protocols and employee education initiatives, leveraging technology-driven approaches such as encryption and multi-factor authentication, ensuring transparency in data acquisition and dissemination, and adopting cybersecurity strategies such as network segmentation and sharing of threat intelligence.

Although the implementation of these solutions presents challenges, healthcare organisations must prioritise patient privacy and security to safeguard patient care from potential compromise. The ramifications of data breaches and cyber threats can be significant, potentially

leading to harm to patients and reputational harm for healthcare institutions.

VI. REFERENCES

1. Bojinov, H., Schinzel, S., &Perrig, A. (2018). Multi-factor authentication for electronic health records: An evaluation of the state-of-the-art. Journal of biomedical informatics, 78, 130-143.
2. Gianfrancesco, M. A., Tamang, S., Yazdany, J., &Schmajuk, G. (2018). Potential biases in machine learning algorithms using electronic health record data. JAMA internal medicine, 178(11), 1544-1547.
3. Kuo, T. T., Kim, H. E., Ohno-Machado, L., & Oh, S. Y. (2019). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 26(10), 1411-1417.
4. Li, X., Shen, C., Hou, T., & Zhang, Y. (2020). A survey of cyber attacks on hospitals and the potential impact of cyber attacks on healthcare in China. BMC public health, 20(1), 1-12.
5. Wang, X., Sun, Q., &Xie, L. (2020). Healthcare data breaches in 2019. Journal of medical systems, 44(8), 1-8.
6. Zhang, P., White, J., Schmidt, D. C., & Lenz, G. (2018). Blockchain technology use cases in healthcare. In Proceedings of the 2018 IEEE International Conference on Healthcare Informatics (pp. 519-520). IEEE.