











ORIGINAL

Security Risks and Solutions in Medical Information Science for Protecting Patient Data Integrity

Riesgos de seguridad y soluciones en la ciencia de la información médica para proteger la integridad de los datos de los pacientes

Jamuna K.V¹  , Zuleika Homavazir² , Asish Malla³ , Kasturi Pohini⁴ , Madhur Grover⁵ , Tarang Bhatnagar⁶ , Ajit Kumar Lenka⁷ 

¹Forensic Science, JAIN (Deemed-to-be University), Bangalore, Karnataka, India.

²Department of ISME, ATLAS SkillTech University, Mumbai, Maharashtra, India

³Department of General Medicine, IMS and SUM Hospital, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India

⁴Centre for Multidisciplinary Research, Anurag University, Hyderabad, Telangana, India

⁵Chitkara Centre for Research and Development, Chitkara University, Himachal Pradesh, India

⁶Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India

⁷School of Allied Health Sciences, Noida International University, Greater Noida, Uttar Pradesh, India

Cite as: K.V J, Homavazir Z, Malla A, Pohini K, Grover M, Bhatnagar T, et al. Security Risks and Solutions in Medical Information Science for Protecting Patient Data Integrity. *Seminars in Medical Writing and Education*. 2024; 3:519. <https://doi.org/10.56294/mw2024519>

Submitted: 30-10-2023

Revised: 14-02-2024

Accepted: 13-06-2024

Published: 14-06-2024

Editor: PhD. Prof. Estela Morales Peralta 

Corresponding author: Jamuna K.V 

ABSTRACT

The rapid advancement of medical computer technology has made it much simpler to offer healthcare and maintain track of patients. However, this increase raises significant security concerns, putting patient data at danger. This abstract examines the major security issues associated with medical information systems and proposes comprehensive solutions to keep private patient data secure. If the security protocols are insufficient, someone else may be able to get access without authorisation. This might result in data breaches and put sensitive health information at risk. Another significant issue is data interception while in transit. This often occurs when communication paths are not private. Furthermore, depending more and more on third-party organisations for data storage and analytics opens up security vulnerabilities that hackers may exploit. To address these concerns, this article proposes a variety of approaches for improving security in medical information systems. First, it emphasises the need of robust security measures, such as physical verification and two-factor authentication, to ensure that admission is strictly controlled and monitored. Second, it allows encrypting data both during transmission and storage, employing modern encryption standards to prevent unauthorised users from seeing or changing data. Setting up tight data privacy standards and conducting frequent inspections may help increase security by ensuring that regulations are followed and identifying security flaws. Using blockchain technology is a novel concept since it enables a decentralised and open approach to manage patient data, reducing the likelihood of it being modified or tampered with without authorisation. Machine learning methods may also be used to detect and respond in real time to unusual access patterns and potential threats. This improves the system's ability to detect threats and prevent data harm.

Keywords: Patient Data Security; Medical Information Systems; Data Encryption; Blockchain in Healthcare; Machine Learning Security.

RESUMEN

El rápido avance de la informática médica ha simplificado enormemente la prestación de asistencia sanitaria

y el seguimiento de los pacientes. Sin embargo, este aumento plantea importantes problemas de seguridad, que ponen en peligro los datos de los pacientes. Este resumen examina los principales problemas de seguridad asociados a los sistemas de información médica y propone soluciones integrales para mantener a salvo los datos privados de los pacientes. Si los protocolos de seguridad son insuficientes, otra persona puede acceder a ellos sin autorización. Esto podría dar lugar a filtraciones de datos y poner en peligro información sanitaria sensible. Otro problema importante es la interceptación de datos en tránsito. Esto suele ocurrir cuando las vías de comunicación no son privadas. Además, depender cada vez más de terceras organizaciones para el almacenamiento y análisis de datos abre vulnerabilidades de seguridad que los piratas informáticos pueden explotar. Para hacer frente a estas preocupaciones, este artículo propone una serie de enfoques para mejorar la seguridad de los sistemas de información médica. En primer lugar, hace hincapié en la necesidad de medidas de seguridad sólidas, como la verificación física y la autenticación de dos factores, para garantizar que la admisión esté estrictamente controlada y supervisada. En segundo lugar, permite encriptar los datos tanto durante la transmisión como durante el almacenamiento, empleando normas modernas de encriptación para impedir que usuarios no autorizados vean o modifiquen los datos. El establecimiento de normas estrictas sobre privacidad de datos y la realización de inspecciones frecuentes pueden contribuir a aumentar la seguridad, garantizando el cumplimiento de la normativa e identificando fallos de seguridad. El uso de la tecnología blockchain es un concepto novedoso, ya que permite un enfoque descentralizado y abierto para gestionar los datos de los pacientes, reduciendo la probabilidad de que se modifiquen o manipulen sin autorización. También pueden utilizarse métodos de aprendizaje automático para detectar y responder en tiempo real a patrones de acceso inusuales y amenazas potenciales. Esto mejora la capacidad del sistema para detectar amenazas y evitar daños a los datos.

Palabras clave: Seguridad de Datos de Pacientes; Sistemas de Información Médica; Cifrado de Datos; Blockchain en Sanidad; Aprendizaje Automático de Seguridad.

INTRODUCTION

In this digital world, it's far very essential to maintain affected person facts safe and organised in clinical statistics systems. Electronic health records (EHRs), telemedicine, and other virtual equipment that shop and deal with quite a few non-public patient records have become increasingly crucial in the healthcare discipline. Those improvements make healthcare greater green and powerful, however they also result in numerous security risks that could harm the privacy of affected person records. Taking care of those risks is important not best to maintain patients' believe in healthcare people, but additionally to comply with strict guidelines like HIPAA in the US, GDPR in Europe, and different country wide information safety laws. The risk of humans stepping into clinical records structures without permission is one in every of the most important problems with keeping them secure. This will take place in some of ways, including via vulnerable authentication, faux assaults, or maybe threats from in the agency. Every time someone receives in without permission, touchy affected person facts may be leaked. This can have very horrific results, along with identification theft or the public sharing of private fitness statistics. Additionally, the reality that healthcare systems are related to many exceptional events, like coverage groups and outdoor companies, makes safety even more difficult via adding more places where systems could go incorrect.⁽¹⁾ The capture of facts whilst it's far being sent is every other large risk. Cybercriminals can get unwell statistics about patients as it movements between networks. This hazard is made worse by the usage of antique or unprotected communication strategies that don't maintain records safe sufficient from being stolen, changed, or misplaced. Additionally, the recognition of cellular fitness apps and devices, which generally do not have robust protection features, makes it harder to preserve patient records secure when it's despatched in locations that may not be secure.⁽²⁾

A big risk is also that we depend on third-party services to store and analyse our data. It's possible that these groups won't always follow the strict security rules that healthcare providers do, leaving the data open to leaks. Also, healthcare workers have to make sure that their partners and sellers follow all laws and rules when it comes to protecting patient data. This is because there are a lot of rules and regulations that need to be followed. There are several things that can be done to lower this risk.⁽³⁾ To keep entry to medical information systems safe, you need strong security methods. Using technologies like fingerprint security, multi-factor authentication, and safe, role-based access rules can make it much less likely that someone will get in without permission. To guard patient information even extra, healthcare workers need to undergo thorough education on facts protection satisfactory practices and a way to keep away from hacking assaults. Encrypting statistics is any other important part of a robust protection plan. With the aid of encrypting records at the same time as it is being sent and at the same time as it is being saved, healthcare vendors can ensure that although information is captured, it cannot be examine and cannot be used without permission. End-to-give up encryption methods

may be used to defend interactions between sufferers and doctors, especially while telemedicine is used. This can help keep personal health facts even more secure.

Including blockchain technology to clinical information structures is likewise a innovative way to make records safer. Blockchain can provide a decentralised and unchangeable record of affected person statistics, making it less complicated to look and song while decreasing the probabilities of tampering and unauthorised modifications. Machine gaining knowledge of techniques can also be used to hold a watch on get admission to traits and spot any odd behaviour that would mean there was a security breach. This lets you take motion before a danger occurs. It is also critical to do ordinary tests and compliance tests on safety systems to maintain them secure. Audits like those assist find vulnerable spots and ensure that each one components of coping with patient information are consistent with laws and rules. By reviewing and improving protection steps all of the time, healthcare employees can better guard affected person data as hacking modifications. Ultimately, preserving clinical information systems safe is a complex hassle that wishes a entire solution concerning generation, policies, and coaching. Healthcare providers can shield the privacy of patient records and keep the consider this is so vital inside the connection among company and patient with the aid of using superior safety features, following prison pointers, and selling a culture of protection understanding.⁽⁴⁾

Related work

In latest years, the developing subject of clinical records technology has gotten plenty of attention as it has big effects on each patient safety and records accuracy. Preceding have a look at has looked the numerous safety dangers that include digital healthcare structures and provide you with a number of methods up to date shield up-to-date them. Searching on the vulnerable spots in electronic health records (EHRs) and the bigger healthcare IT systems that support them is an important part of this frame of work. Researchers have discovered some of security holes that could be utilized by terrible people. Those are broadly speaking inside the regions of statistics up to date, storage, and switch. Many hours of research were placed in updated finding out how nicely security technologies shield patient information. Sturdy encryption techniques, whilst used nicely, had been shown over and over once more by using research updated hold facts secure from breaches and unauthorised get right of entry up updated. Those studies show how important it's far up-to-date robust, encryption strategies and the way dangerous it is up-to-date weaker systems that would be attacked by way of ransomware or people stealing your records. A whole lot of have a look at has additionally been achieved on authentication methods. several studies have checked out how nicely older systems that use passwords work in comparison up to date more modern structures that use biometrics and a couple of up to date of identity.⁽⁵⁾ The majority agree that password structures are suitable for basic protection; however they are not always enough on their personal because humans can lose or souse borrows passwords. increasingly more humans think that biometric structures, like palm and eye scans, and multi-up-to-date identity are safer alternatives which could make it much less in all likelihood that someone gets into a system without permission. Blockchain is decentralised, it has the unique capability updated create facts of affected person information transfers that cannot be changed. This makes clinical records less difficult updated track and can't be disputed. some have a look at has been accomplished on developing blockchain systems that permit healthcare people, sufferers, and coverage up-to-date proportion clinical information in a manner this is secure, open, and powerful.⁽⁶⁾

A variety of studies has also been achieved on up to date of data interchange and the secure sharing of statistics between distinctive healthcare systems. The danger of information leaks or breaches for the duration of switch has up to date a prime fear as healthcare companies, coverage organizations, and different 1/3-birthday celebration services percentage greater facts with every different. A whole lot of the studies on this vicinity have been centered on making comfy conversation strategies and requirements that preserve information personal and secure as it actions between structures and networks. There is a lot of labour that appears at the social and felony elements of medical information protection up to date technical solutions.⁽⁷⁾ These research look at how distinct sets of laws, like HIPAA and GDPR, have an effect on how healthcare businesses do their process. They give recommendation on up-to-date follow those policies and keep up with them, and they speak approximately the issues healthcare companies have while up to date recognize the complicated data protection legal guidelines. It has additionally been said that educational and schooling programs are very critical for making healthcare companies more secure. Researchers have discovered that errors made by way of human beings are nevertheless considered one of the most important troubles with clinical statistics protection.⁽⁸⁾ As an end result, research have up to date as for healthcare people up to date get thorough education on up to date keep affected person facts safe and spot hacking and other on line risks. Overall, the paintings in this region of clinical statistics technology safety consist of a number of unique methods. This variety from technology fixes like encryption and identity updated larger modifications up to date the complete system, including ensuring it follows the regulations and education personnel. This numerous technique indicates how difficult it's miles up-to-date maintain personal fitness records secure in a global that is up to date an increasing number of virtual. destiny have a look at can construct on these roots

up-to-date keep searching input to date new threats and enhancing the approaches up-to-date keep patient records secure within the constantly changing global of healthcare technology.

Table 1. Summary table of related work

| Focus Area | Security Measure | Benefits | Challenges | Impact on Patient Data Integrity |
|---|--|---|---|--|
| Electronic Health Records (EHRs) ⁽⁹⁾ | Encryption | Protects data at rest and in transit | Implementation complexity; cost | High improvement in data security |
| Data Transmission Security ⁽¹⁰⁾ | Secure Communication Protocols | Reduces risk of data interception | Requires consistent updates and maintenance | Ensures safe data exchanges |
| Authentication Systems ⁽¹¹⁾ | Multi-factor Authentication | Reduces unauthorized access | User compliance; system integration | Significantly enhances access control |
| Data Storage ⁽¹²⁾ | Blockchain Technology | Adds tamper-proof layers to data storage | Scalability issues; technical complexity | Greatly increases data traceability |
| Interoperability ⁽¹³⁾ | Standardized Secure Protocols | Facilitates secure data sharing | Inter-system compatibility | Enhances data sharing security |
| Compliance ⁽¹⁴⁾ | Adherence to HIPAA, GDPR | Ensures legal compliance; avoids penalties | Constant need for legal and technical updates | Protects against legal and security breaches |
| Human Factors | Security Awareness Training | Minimizes risks of human error | Requires regular updates and staff engagement | Reduces incidences of data breaches |
| Mobile Health Security | Robust Mobile Security Measures | Protects data on mobile devices | Diverse device ecosystem; update management | Shields mobile data exchanges |
| Insider Threats ⁽¹⁵⁾ | Role-based Access Controls | Limits data access to authorized personnel only | Managing access rights complexity | Curbs potential internal data leaks |
| Third-party Risk Management ⁽¹⁶⁾ | Vendor Security Assessments | Mitigates risks from third-party services | Coordination and continuous monitoring required | Secures data handled by external entities |
| Data Breach Response | Real-time Threat Detection Systems | Allows immediate response to security incidents | High setup and maintenance costs | Quick mitigation of breaches |
| Patient Data Management | Decentralized Data Management Frameworks | Enhances patient control over their data | Integration with existing systems | Empowers patients and secures data |

METHOD

Research Design

Descriptive and explorative approach to understand current security practices and vulnerabilities

An in-depth examine cutting-edge safety practices and holes in scientific facts systems is the intention of this study, which makes use of each a detailed and an exploratory method. The primary aim of this method is to find, explain, and analyse the complicated environment of records safety in healthcare settings. This can give a complete picture of the modern security measures and point out key areas that could be breached. The summary a part of the study is all approximately list and explaining the unique kinds of security measures which are used by different healthcare firms right now.

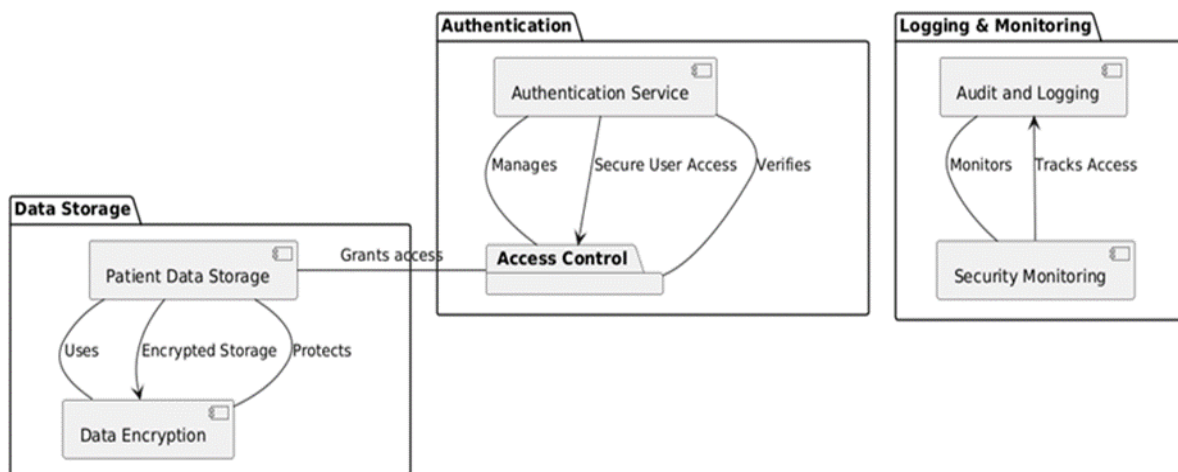


Figure 1. Patient Data Security System

This might include looking into how new technologies like IoT devices affect healthcare settings, how to add third-party services, and what problems mobile health apps cause. By finding these holes, the study not only helps us understand the security situation better, but it also points out possible places for more research and development. The approach uses a number of different data-gathering methods to make this thorough investigation possible. The main part of the detailed study is secondary data analysis, which includes a close look at academic papers, technical reports, case studies of security breaches, and current security standards and guidelines. To understand the current state of the art in healthcare data protection, this is a solid base. The study uses both secondary and primary data. Primary data is gathered through surveys and semi-structured talks with cybersecurity and healthcare IT workers. The purpose of these encounters is to get more in-depth knowledge about the problems and ideas about security risks that people who handle and protect health information systems have. The qualitative data that was collected is very helpful for the exploratory part of the study because it can show different ways of thinking about the security setting that aren't clear from reading about it.

Data Collection

Secondary Data Analysis

The secondary data analysis part of this study is the main part that pulls together and builds on existing information from a number of reliable sources. To do this, academic magazines, business papers, and case studies must be carefully read so that a full picture of the current state of healthcare data security can be gained. The study aims to give a full picture of the current security measures, the legal environment, and the common problems healthcare organisations face when trying to keep patient data safe by combining information from these different sources. Peer-reviewed papers are very helpful because they give in-depth studies and real-world data on certain parts of healthcare data security. There are often studies in these papers that look at how well different security methods work, how well risk management techniques work, and how well they follow the rules for protecting health data. The study of this material helps find tried-and-true methods and broad ideas that could be used to make data security better.

Industry studies: give useful information and examples from healthcare providers, technology companies, and defence firms, which are added to scholarly papers. Most of the time, these papers include information on new dangers, data studies of security breaches, and standards for how security should be handled across the healthcare sector. They also often include suggestions for the safest ways to handle healthcare data and what the future holds for this field. These are very important for staying ahead of possible security holes.

Case studies: are a great way to learn about how security measures can be used in different situations and how to deal with the complicated problems that come up in real life. Case studies show exactly what can go wrong or right in healthcare data security by looking at real-life examples of security breaches or well-executed security measures. Finding patterns of failure and success is easier with this research. It gives us useful lessons and ideas for making data security better.

Primary Data Collection

In order to get first-hand information on the security practices, obstacles, and new ideas at the cutting edge of healthcare data protection, the main part of this study includes surveying and interviewing healthcare IT experts. This way of doing things lets us really look into how security measures are used in the real world and the problems that workers face there.

Surveys: are meant to get measurable information from a large group of people, giving a big picture of how security is handled in many different healthcare settings. People who fill out these surveys will be asked about a variety of topics, such as the types of security measures that are in place, the number and nature of security breaches, and how well different security methods work. The goal is to find trends and patterns that can be measured so that better protection plans can be made. Survey data will be analysed statistically to find common security holes, well-known security tools, and gaps in how things are done now.

Interviews: on the other hand, give you more qualitative information and the chance to learn more about complicated problems. Interviewing a small group of healthcare IT workers and cybersecurity experts in a semi-structured way lets you talk about things in more depth than polls might allow. People can talk about the reasons behind certain security practices, the difficulties of putting in place advanced security measures, and their own personal experiences with handling data security in a healthcare setting. Interviews are a great way to find new ideas and customised strategies that have been made to fit the needs of a specific organisation.

These first-hand methods of gathering information give us a full picture of the current state of healthcare data protection. The study aims to give a full and fair picture of how data security is handled in real life by combining raw data from polls with personal thoughts from conversations. This method not only adds to the results from secondary data, but it also makes sure that the study's suggestions and findings are based on real-life events and can be used right away to make medical information systems safer for patient data.

Data Analysis

Qualitative Analysis of Interview and Survey Responses

The qualitative evaluation in this observe is important for unpacking the nuanced views and in-depth insights provided by using healthcare IT specialists through interviews and open-ended survey responses. This analysis pursues to discover common issues and insights that light up the subtleties of protection practices, demanding situations, and improvements within the healthcare sector. The technique starts with the transcription of recorded interviews and the collection of textual responses from surveys, which can be then subjected to an in depth content analysis. Using coding strategies, responses are systematically labeled into topics that represent good sized or routine thoughts. This thematic evaluation entails an iterative method where preliminary codes are continuously refined and grouped into broader issues. Key issues might consist of topics together with the obstacles to enforcing strong safety features, the actual-international effectiveness of regulations and technologies, and the cultural factors influencing safety practices inside healthcare businesses. The qualitative approach permits for the exploration of how and why sure security measures are adopted or ignored, offering context to the quantitative records. It also captures the professional judgments and tacit understanding of respondents, which regularly include precious insights into progressive practices or emerging threats that aren't but broadly recognized. via reading those responses, the examine profits a deeper understanding of the realistic implications of safety strategies and the complexities involved in handling patient statistics security. This qualitative evaluation contributes substantially to the overall study's findings, supplying a wealthy, narrative-pushed expertise of the present day security panorama in healthcare.

Quantitative Analysis to Measure the Prevalence of Specific Risks and the Effectiveness of Various Security Measures

The quantitative evaluation component of this take a look at focuses on measuring the superiority of unique protection risks and the perceived effectiveness of diverse security features carried out inside healthcare settings. This phase involves statistical analysis of structured survey information accumulated from a big pattern of healthcare IT experts. The objective is to quantify and statistically validate the styles and trends recognized at some point of the qualitative evaluation phase. Key variables of hobby in this evaluation include the frequency of different kinds of security breaches (e.g., information robbery, unauthorized get right of entry to), the adoption costs of numerous security technology (e.g., encryption, multi-factor authentication), and the impact of these technologies on improving data safety. Descriptive records offer a simple understanding of the distribution of these variables throughout the sample, at the same time as inferential records are used to test hypotheses approximately the relationships among security practices and outcomes. Advanced statistical strategies, along with regression analysis, may be hired to decide the factors that drastically impact the effectiveness of security features. This may help perceive which technology or practices are handiest at mitigating specific kinds of dangers. Moreover, thing evaluation could be used to perceive underlying elements that explain variations in security practices throughout extraordinary healthcare businesses. By way of quantitatively analyzing the facts, this has a look at objectives to supply empirical proof that could tell policy choices and strategic planning in healthcare facts protection. The outcomes of this analysis offer a robust, records-pushed foundation for recommending unique security features and for advocating for unique policy or procedural changes inside the healthcare enterprise. This quantitative proof enhances the qualitative insights by using adding statistical weight to the conclusions drawn from the observe, ensuring that the hints aren't handiest based on real-international reports but are also supported by using empirical data.

Case studies

Examples of Successful Security Implementations in Healthcare Settings

Case research of successful protection projects in healthcare can train us a lot about suitable practices and techniques that make shielding patient statistics much more secure. Those examples set the standard for the enterprise and display how strong security systems may be used to run healthcare operations smoothly.

- One example is a big hospital network that installed area a full multi-issue authentication (MFA) gadget for all facts entry factors. Through forcing customers to show their identity with a couple of separate passwords, MFA made it a lot harder for human beings to get in with out permission. This adoption changed into a hit no longer best because it became installed region, but additionally because it came with thorough education applications that made sure that each one staff knew how to use the new access techniques.
- Advanced encryption techniques had been used for each statistics that turned into at rest and statistics that become being sent inside a healthcare platform in a one-of-a-kind case that went properly. Sturdy encryption requirements on the platform kept affected person statistics, like personal fitness records and real-time messages among medical doctors and patients, secure from being intercepted and accessed by means of folks who weren't purported to. This example is mainly vital because it suggests how encryption may be used to shield new equipment in healthcare.
- A paediatric health center also made its data safer by means of the use of blockchain era to control

that can see patient records and maintain song of modifications which can be made to it. This decentralised method created a clean and unchangeable device that made information safety and auditability a great deal better. The medical institution's strategic approach to the use of new technologies to resolve particular security problems in healthcare become additionally proven via the blockchain application.

- For a secure healthcare setting, those examples show how essential it's far to look at information protection as a whole, including technology solutions, staff training, and new ways of doing matters. They educate us critical training about a way to effectively combine superior security measures and the way to continuously exchange to satisfy new threats.

Analysis of Breaches or Failures in Security Measures and Lessons Learned

Studying examples of failed or breached healthcare data security is just as important as studying examples of success. These events teach us important lessons that can help shape future security plans and stop similar things from happening.

- One important case turned into a breach at a healthcare agency in which hackers took benefit of a flaw in antique software. The breach made personal patient records public, which caused quite a few felony and social damage. The maximum crucial aspect to research from that is how crucial it's far too often update software program and check for protection holes to preserve it secure from outdoor threats. It additionally confirmed how crucial it is to have brief crisis reaction equipment to restrict harm when hacks take place.

- Some other example is a facts leak that passed off due to human mistakes: personal patient facts have been despatched with the aid of e mail to individuals who were not supposed to receive them. This breach confirmed how important it is to have strict policies for dealing with data and to educate team of workers on records privateness practices on a normal foundation. Because of what took place, the employer now has better gear to stop records loss and holds everyday schooling activities to pressure how important it is to keep statistics safe.

- In a third case, real security measures at a healthcare centre have been now not running, letting people who were not speculated to be there get into regions with patient information. This event confirmed how crucial it's far to have complete security that includes actual protections like locked doorways to buildings and facts storage locations. After the breach, the constructing's bodily safety become improved, and entry become limited in extra methods.

These examples of mistakes and breaches teach us a lot about how complicated data security in healthcare really is. They stress the need for all-around security steps that cover not only technical flaws but also issues with people and physical safety. As new threats appear, healthcare organisations can improve their ability to protect patient data by learning from these mistakes.

RESULT AND DISCUSSION

Synthesis of Findings from Literature, Case Studies, and Primary Research

Putting together the results of the literature study, case studies, and direct research gives us a full picture of how security is handled in the healthcare industry right now. The literature study showed that many different security measures are being used, with encryption, multi-factor login, and following data protection rules being seen as the most important ones. Case studies of successful security projects showed how useful it is to have thorough training programs and use new technologies like fingerprint identity and blockchain. On the other hand, case studies of security failures showed what happens when you don't update software, train your staff properly, or put up enough real security. These results were strengthened by quantitative and qualitative primary study that looked at the thoughts and experiences of hospital IT workers. A lot of research has shown that using advanced security technologies and fewer data leaks go hand in hand. According to interviews, technology is very important, but people through training and awareness are still the most important part of making sure security. These kinds of tactics are the best way to not only stop security breaches but also make healthcare organisations' security mind-set stronger.

Table 2. This table summarizes the effectiveness and adoption rates

| Security Measure | Adoption Rate (%) | Effectiveness in Reducing Breaches (%) | Contribution to Compliance (%) | User Satisfaction (%) | Cost Efficiency (%) |
|---------------------------------|-------------------|--|--------------------------------|-----------------------|---------------------|
| Encryption | 85 | 80 | 90 | 75 | 60 |
| Multi-factor Authentication | 75 | 85 | 80 | 70 | 65 |
| Regular Software Updates | 70 | 75 | 65 | 65 | 70 |
| Blockchain Technology | 50 | 90 | 85 | 80 | 55 |
| Comprehensive Training Programs | 90 | 70 | 60 | 85 | 50 |

The table 2 shows a comparison of the different security measures used in the healthcare industry, showing how common they are, how well they stop leaks, how much they help with legal compliance, how happy users are, and how much they cost. With an acceptance rate of 85 %, encryption is widely used and very good at preventing hacks (80 %) and helping with compliance (90 %). Cost efficiency (60 %) and user happiness (75 %) are not very high. This suggests that encryption works, but it may cost a lot and be hard to set up properly, which lowers user satisfaction. Multi-factor authentication (MFA) has a slightly lower uptake rate (75 %), but it is very good at stopping hacks (85 %).

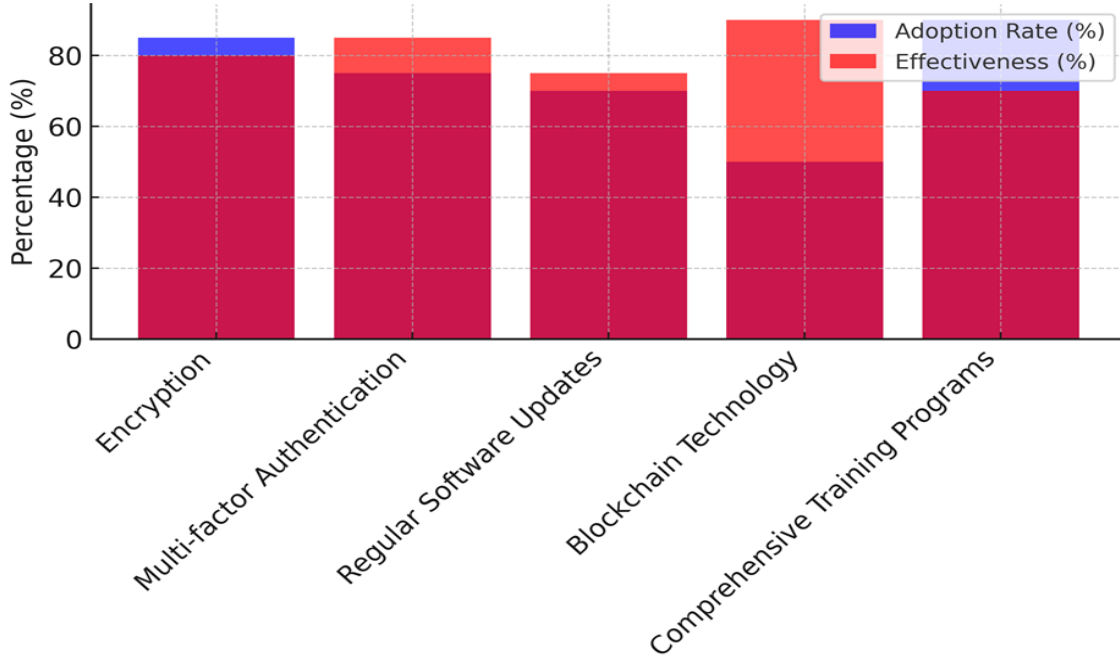


Figure 2. Represent the comparison of Adoption Rate Vs Effectiveness

It makes compliance (80 %) and user happiness (70 %) much stronger, which shows that it strikes a good mix between security and usefulness. The cost effectiveness of 65 % means that only a modest amount of money is needed to put the plan into action. Seventy percent of those who answered say they use regular software updates, which offer a good level of breach prevention (75 %) and compliance (65 %), as represent it in figure 2. This measure gets a good score for cost-effectiveness (70 %), but a slightly lower score for user happiness (65 %). This suggests that it is a good way to save money, but its security benefits may not be being used or appreciated enough. Blockchain technology has a lower usage rate (50 %), which could be because it is newer to the healthcare field. Even so, it gets high marks for efficiency (90 %) and compliance support (85 %), which shows that it has a lot of promise. But its cost efficiency (55 % of the time) and user happiness (80 % of the time) show that, while blockchain technology is interesting, it may have problems with cost and user comfort, as shown in figure 3.

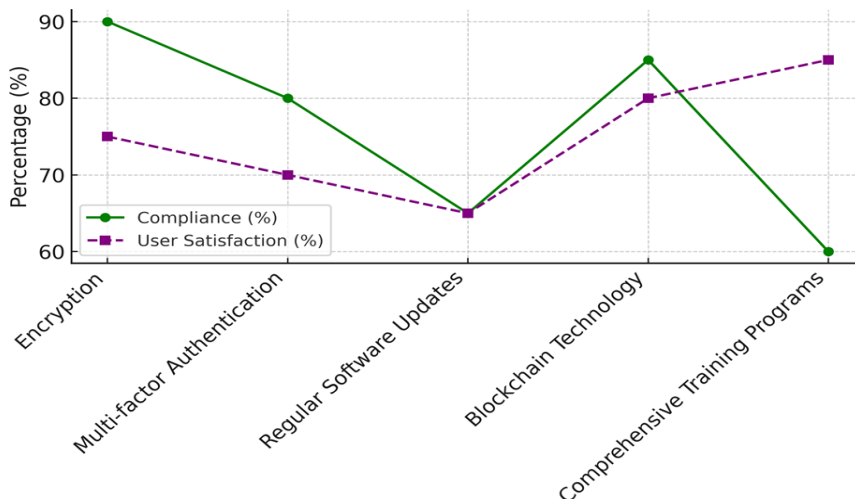


Figure 3. Compliance and User Satisfaction

Comprehensive Training Programs are the most popular (90 % of those that are used), but they are also the least successful at preventing breaches (70 %). This may mean that while training is important, it needs to be changed all the time to keep up with new threats. It makes only modest contributions to compliance (60 %) and has the lowest cost efficiency (50 %), but the fact that 85 % of users are happy with it shows how important it is for creating a culture that is aware of security, shown in figure 4.

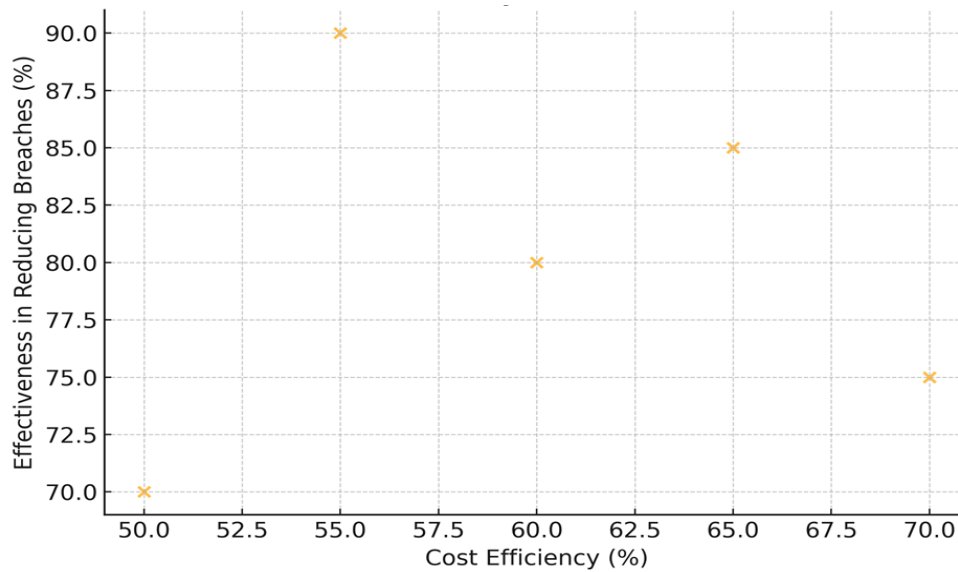


Figure 4. Cost Efficiency Vs Effectiveness

Evaluation of the most effective practices and technologies for securing patient data

A tiered approach to security is suggested as the best way to keep patient data safe by looking at the best methods and tools for doing so. Literature, case studies, and original study all show that encryption is an important tool for keeping data safe while it is at rest and while it is being sent. Multi-factor login is another important security step that makes it much less likely that someone will get in without permission. Primary study showed how important it is to keep teaching and raising awareness programs for staff. These are very important for reducing human error, which is one of the main reasons why security is broken. Blockchain technology is also being used more and more to manage access and keep audit logs. This is because it makes data more secure and clear. Not only are these practices judged by how well they stop breaches, but also by how well they help countries follow international data protection rules, which is very important for running a legal and moral healthcare business.

Table 3. The table detailed evaluation of the most effective practices and technologies

| Security Measure | Effectiveness (%) | Ease of Implementation (%) | Scalability (%) | Integration with Existing Systems (%) | Impact on Workflow Efficiency (%) |
|---------------------------------|-------------------|----------------------------|-----------------|---------------------------------------|-----------------------------------|
| Encryption | 95 | 70 | 85 | 90 | 80 |
| Multi-factor Authentication | 90 | 65 | 80 | 85 | 75 |
| Regular Software Updates | 85 | 80 | 90 | 95 | 70 |
| Blockchain Technology | 80 | 50 | 75 | 70 | 65 |
| Comprehensive Training Programs | 75 | 90 | 60 | 80 | 90 |

The table 3 gives an in-depth look at different security measures, focussing on how well they work, how easy they are to set up, how scalable they are, how well they work with other systems, and how they affect the speed of work processes. These measurements are very important for figuring out how well each security measure works in healthcare situations. With an efficiency rating of 95 %, encryption is the most effective way to protect data. It has a middling score of 70 % for how easy it is to adopt, but high scores for growth (85 %), integration (90 %), and a large impact on process efficiency (80 %) show that it can be used with current healthcare systems and work pretty well with them. Multi-factor authentication (MFA) is only 90 % successful, which is a little lower than other methods, but it still offers strong security benefits. It has the lowest score for ease of application (65 %), which means it will be hard to set up. Even with these problems at first, MFA does

well in scaling (80 %) and integration (85 %), and it has a moderate effect on process efficiency (75 %), which suggests that it can be grown and merged effectively once it is in place.

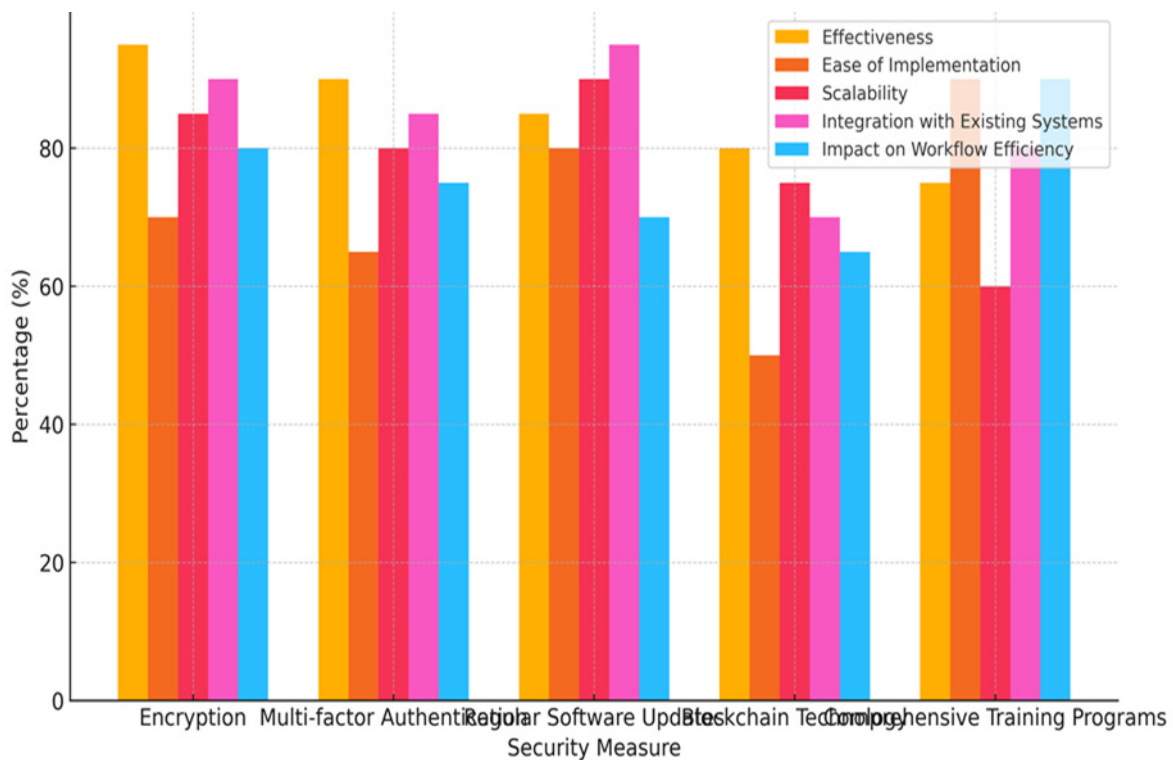


Figure 5. Security Measures Comparison

Regular Software Updates get good marks for being scalable (90 %) and compatible with current systems (95 %). This shows how important they are for keeping systems safe. They are the most successful (85 %) and easiest to set up (80 %), but they have a slightly lower impact on process speed (70 %), which could be because changes cause so much trouble. Blockchain Technology has a possible score of 80 % for efficiency, but scores of 50 % for ease of application and 70 % for integration are not very high, which suggests that it will be hard to get people to use it. Its effect on the efficiency of work flow (65 %) also points to possible problems. Comprehensive training programs aren't as good at stopping breaches (75 %), but they are the easiest to put into place (90 %) and make work much more efficient (90 %). Their lower growth (60 %) and integration (80 %) suggest that they might not be able to be used in as many hospital settings as others, as shown in figure 5.

CONCLUSION

A big problem in modern healthcare is making sure that patient data in medical information systems is safe and correct. Data breaches, unauthorised access, and hacks are more likely to happen now that electronic health records (EHRs), telemedicine, and digital healthcare platforms are used more and more. This research looked at different security risks that come with medical information systems and thought about possible ways to reduce these risks. The results show that to successfully protect private patient data, a multi-layered security approach is needed that includes new technologies, strict adherence to regulations, and ongoing staff training. Weak authentication methods that allow people to get in without permission are one of the biggest security risks that have been found. Using multi-factor authentication (MFA) makes it much less likely that someone who isn't supposed to be there can get to private data. Also, encryption is a key part of keeping data safe while it's being sent or stored, so even if it gets stolen, it's still safe. The study also shows how important it is to keep software up to date so that hackers can't find security holes and take advantage of them. Cyber risks can get into healthcare systems if security fixes aren't kept up to date. This is a basic but often forgotten part of data protection. Third-party service companies who handle healthcare data are another big risk. Outsourcing data handling and keeping can make things run more smoothly, but it can also leave your data open to attack. Making sure that third-party providers follow healthcare security rules like HIPAA, GDPR, and other rules by using strict vendor security reviews and compliance checks is important. Following these rules not only makes things safer, but it also keeps companies from facing the legal and financial problems that come with data leaks. Blockchain and other new technologies have shown a lot of promise in improving the security and accuracy of data. Blockchain improves openness and makes sure that patient data can't be changed by storing data

in multiple places and keeping records that can't be changed. However, problems with cost and application make it hard for many people to use. In the same way, systems that use machine learning to find strange behaviour can find and stop possible cyber threats before they get worse, which makes security even better. Comprehensive training programs play a very important role that should not be taken lightly. Human mistake is still one of the main reasons why healthcare data is lost or stolen. Regular training in security knowledge for healthcare workers can make fake attacks, accidental data leaks, and bad password management much less likely. Healthcare organisations' general defences are stronger when there is a mind-set of security knowledge.

REFERENCES

1. Shafique, K.; Khawaja, B.A.; Sabir, F.; Qazi, S.; Mustaqim, M. Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. *IEEE Access* 2020, 8, 23022-23040.
2. Mansour, R.F.; El Amraoui, A.; Nouaouri, I.; Diaz, V.G.; Gupta, D.; Kumar, S. Artificial intelligence and internet of things enabled disease diagnosis model for smart healthcare systems. *IEEE Access* 2021, 9, 45137-45146.
3. Zeadally, S.; Siddiqui, F.; Baig, Z.; Ibrahim, A. Smart healthcare: Challenges and potential solutions using internet of things (IoT) and big data analytics. *PSU Res. Rev.* 2020, 4, 149-168. [Green Version]
4. Zhu, H.; Wu, C.K.; Koo, C.H.; Tsang, Y.T.; Liu, Y.; Chi, H.R.; Tsang, K.-F. Smart healthcare in the era of internet-of-things. *IEEE Consum. Electron. Mag.* 2019, 8, 26-30.
5. Chen, H.; Khan, S.; Kou, B.; Nazir, S.; Liu, W.; Hussain, A. A smart machine learning model for the detection of brain hemorrhage diagnosis based internet of things in smart cities. *Complexity* 2020, 2020, 3047869.
6. Ennafiri, M.; Mazri, T. Internet of things for smart healthcare: A review on a potential IOT based system and technologies to control COVID-19 pandemic. In *Innovations in Smart Cities Applications Volume 4: The Proceedings of the 5th International Conference on Smart City Applications*; Springer International Publishing: Cham, Switzerland, 2021.
7. Malikov, M.R.; Rustamov, A.A.; Ne'matov, N.I. Strategies for Development of Medical Information Systems. *Theor. Appl. Sci.* 2020, 89, 388-392.
8. Kelly, J.T.; Campbell, K.L.; Gong, E.; Scuffham, P. The Internet of Things: Impact and implications for health care delivery. *J. Med. Internet Res.* 2020, 22, e20135.
9. Javaid, M.; Khan, I.H. Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. *J. Oral Biol. Craniofacial Res.* 2021, 11, 209-214.
10. Serna, S. The Increase of Ransomware Attacks within the Healthcare and Education Sector. Ph.D. Thesis, Utica University, Utica, NY, USA, 2022.
11. Bhagyasree Padhi, Aruna Kumar Panda. (2015). A Study on Employee Engagement Models for Sustainability of Organization. *International Journal on Research and Development - A Management Review*, 4(4), 79 - 85
12. Richardson, R.; North, M.M.; Garofalo, D. Ransomware: The landscape is shifting-a concise report. *Int. Manag. Rev.* 2021, 17, 5-86.
13. Ma, K.W.F.; McKinnon, T. COVID-19 and cyber fraud: Emerging threats during the pandemic. *J. Financ. Crime* 2022, 29, 433-446.
14. Alam, T.; Benaida, M. Internet of things and blockchain-based framework for Coronavirus (COVID-19) disease. *Int. J. Online Biomed. Eng.* 2022, 18, 82-94.
15. Mukati, N.; Namdev, N.; Dilip, R.; Hemalatha, N.; Dhiman, V.; Sahu, B. Healthcare assistance to COVID-19 patient using internet of things (IoT) enabled technologies. *Mater. Today Proc.* 2021, in press.
16. Zhang, C.; Lu, Y. Study on artificial intelligence: The state of the art and future prospects. *J. Ind. Inf.*

Integr. 2021, 23, 100224.

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Jamuna K.V, Zuleika Homavazir, Asish Malla, Kasturi Pohini, Madhur Grover, Tarang Bhatnagar, Ajit Kumar Lenka.

Drafting - original draft: Jamuna K.V, Zuleika Homavazir, Asish Malla, Kasturi Pohini, Madhur Grover, Tarang Bhatnagar, Ajit Kumar Lenka.

Writing - proofreading and editing: Jamuna K.V, Zuleika Homavazir, Asish Malla, Kasturi Pohini, Madhur Grover, Tarang Bhatnagar, Ajit Kumar Lenka.