THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 5. Issue 4 (2025)
https://doi.org/10.62019/vdpf0821

An Efficient Big Data Security and Privacy in Healthcare for Enhancing Remote Sensing and Monitoring: A Technological Perspective based on ACL for Preserving Big Data Analytics in Cloud

Irfan Farooq*, Umair Ghafoor, Sania Umer, Arshad Ali, Abdul Karim Shahid, Hamayun Khan

Chronicle

Article history
Received: Oct11, 2025
Received in the revised format: Nov 22. 2025
Accepted: Nov 28, 2025
Available online Dec 22, 2025

Irfan Farooq, is currently affiliated with the Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan.
Email: irfanfarooq9@gmail.com

Umair Ghafoor, is currently affiliated as Deputy Head of Engineering Calrom Limited, M1 6EG, United Kingdom.
Email: umairghafoor@hotmail.com

Sania Umer, is currently affiliated with the Comsats University Islamabad, Wah Campus, Wah cantt, Pakistan
Email: saniaumer554@gmail.com

Arshad Ali, is currently affiliated with the Faculty of Computer and Information Systems, Islamic University of Madinah, Al Madinah Al Munawarah, 42351, Saudi Arabia.
Email: a.ali@iu.edu.sa

Abdul Karim Shahid
Department of Computer Science, COMSATS University, Lahore Campus
Email: akarim@cuilahore.edu.pk

Hamayun Khan is currently affiliated with the Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan.
Email:
hamayun.khan@superior.edu.pk

Corresponding Author*

Abstract

The growing adoption of big data technologies in healthcare has significantly enhanced patient care, diagnostics, and system efficiency. Yet, this transformation brings with it serious concerns about the security and privacy of sensitive medical information. The health care industry is in a critical phase of intelligence with the rapid advancement of modern information technology. With the increased use of healthcare big data, the issue of information security is increasingly becoming critical in the management of smart healthcare care, including the leak of patient privacy, the most critical issue. Thus, the enhancement of information management of intelligent health care during the age of big data is a significant aspect of long-term sustainable development of the hospitals. This paper has initially determined the most influential indicators to influence the privacy disclosure of big data in managing health care and presented a comprehensive overview of the current landscape in healthcare data security and thereafter set the privacy and security based access control model, which has been applied on the security and management of big data in utilization of medical data, and solves the issue of actual data breach where actual problems are involved. Lastly, the model is contrasted with the state-of-the-art techniques. The paper offers a comparative analysis of proposed solutions, considering numerous parameters and highlighting critical gaps for building more secure and trustworthy healthcare systems. The findings confirm that the model is useful in the evaluation of the existing safety threats and forecasting the scope of the various risk factors, by demonstrating that Network Segmentation and Cloud Usage (Hybrid) have significantly enhanced the results by 1.5% and 6.7% respectively and the User Access mechanism is upgraded by 1.5% and 6.7% respectively. The Audit Trail and Compliance is also improving as the proposed technique examines ACL and explores key global regulatory frameworks like the GDPR and HIPAA. The outcome of this study suggests that the proposed access control model is resistant to most cyber-attacks in big data, and it is also demonstrated that the offered framework can be used as a starting point in order to develop secure and safe medical big data solutions. Therefore, this study can be valuable to future scholars to understand the information about the security and privacy of big data in the medical field and ways to implement countermeasures.

Keywords: Big Data, Healthcare, Data Security, Privacy Protection, Blockchain, Anomaly Detection, GDPR, HIPAA, Federated Learning, Encryption Techniques.

INTRODUCTION

The contemporary healthcare system produces enormous amounts of data from various sources. They are electronic health records (EHRs), medical imaging systems, lab results, wearable health monitors, mobile health apps, insurance claims and, most recently, genomics data [1]. It is this heterogeneous combination of structured and unstructured data, which encompasses the patient demographics and diagnostic codes, but goes all the way up to the continuous biometric streams to what is known as big data in healthcare [2]. Big data presents radical possibilities in medicine. It allows making diagnoses more accurately, supporting predictive analytics, providing patients with an opportunity to detect diseases at an early stage, managing the health of the population, and improving clinical decision-making. Nevertheless, storing and controlling such large volumes of sensitive data is extremely demanding in terms of technical and ethical factors [3, 4]. The healthcare system's big data lifecycle can be generally broken down into five steps that are essential: data collection, storage, analysis, utilization, and destruction. There are vulnerabilities presented by each stage. As an example, when collecting data, the data sent by IoT-based devices, such as fitness trackers or smart medical sensors, may be compromised because of the insecure transmission protocols [5]. As soon as they have been gathered, the information is stored in centralized or cloud-based repositories that are frequently targeted by cybercriminals because of the high price of medical records [6].

Big Data in Healthcare

During the analysis stage, privacy issues may occur when the information gets exchanged between institutions or third parties who are contracted to analyze it, particularly in cases where their anonymization measures are not very strong or reversible[7]. At the stage of utilization, the problem of unauthorized access or abuse of data by the internal staff or malicious actors is one of the major concerns. Lastly, at the destruction or archival stage, there may still be residual risk in the presence of remnants of sensitive data in case of improperly sanitized or deleted data [8]. Equations 1, 2 and 3 show the function ELU – E- Linear Unit with 0 < a is

$$f(x) = \begin{cases} \alpha(\exp(x) - 1) & \text{for } x < 0 \\ x \text{ for} & x \geq 0 \end{cases} \quad \text{Eq (1)}$$

$$\delta_h = 60^{\circ} \begin{cases} 0 + \frac{(\beta_g - \beta_b)}{(m_x - m_n)}, if m_x = \beta_r \\ 2 + \frac{(\beta_b - \beta_r)}{(m_x - m_n)}, if m_x = \beta_g \\ 4 + \frac{(\beta_r - \beta_g)}{(m_x - m_n)}, if m_x = \beta_b \end{cases} \quad \text{Eq (2)}$$

These challenges are further complicated by the need to comply with national and international privacy laws, maintain data integrity, and ensure system availability [9, 10]. Figure 1 illustrates the varying levels of security risk associated with each phase of the data lifecycle, underscoring the importance of a comprehensive, end-to-end approach to big data protection in healthcare [11, 12]. Big Data is not a new term, as it was first used in the early 1990s, but its origin is somewhat obscured. The concept of large data work was just starting to develop [13, 14]. Nowadays, Big Data is omnipresent, as it helps drive your favorite applications, helps physicians make faster and more precise diagnoses, informs the business approach, and enhances scientific research [15].

$$\delta_s = \left(\frac{m_x - m_n}{m_n} \right)$$ Eq (3)

$$\delta_v = m_x(\beta_r, \beta_g \beta_b,),\ \delta_{sv} = m_n(\beta_r, \beta_g \beta_b,)$$ Eq (4)

To have a clear picture of what Big Data is, one can consider it to be a combination of statistics, mathematics, and computer science. People have been collecting data to understand the world since ancient times, tracking the crops, the population, or even the disease trends. The only difference now is that the amount of information we produce each day via clicks, swipes, sensors and other digital interactions is vast, coupled with the enormous processing capabilities that we have achieved through powerful computing systems, as illustrated in R(t) function under centric big data volume Equation 5, 6 and 7 [16, 17]. In the simplest terms, Big Data is simply a contemporary expansion of our age-old need to understand patterns and predict results, only to be scaled to the pace and complexity of our modern world. Increased speed and intelligence in technologies and their tools of analysis allow us to discover trends, predict difficulties, and find solutions to problems that would have been considered unthinkable within a few decades past [18, 19].

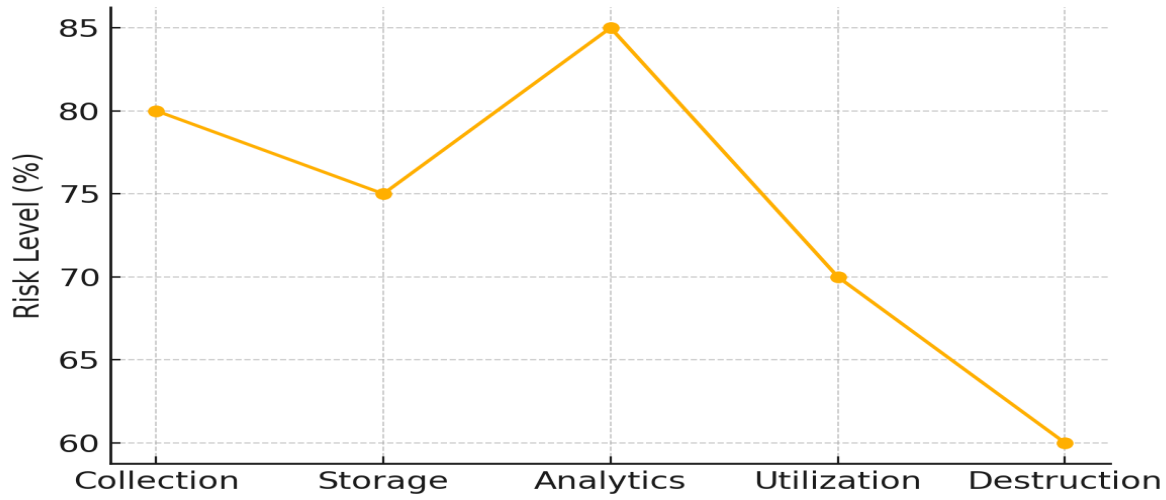

Figure 1.
Big Data lifecycle stages and corresponding security risks.

Big Data in Healthcare

The purpose of the study is to facilitate an engaging discourse on the topic of Big Data security and privacy, particularly in the context of the healthcare industry, by defining the common vocabulary. It brings out important concepts and describes their relationship with larger standards and technologies [20, 21]. Which is the practical value of the analytics knowledge; Security and Privacy of Big Data, noting the necessity of scalable, secure computing systems able to operate large and sensitive data sets [22] Cloud Computing, the ability to access shared computing resources on demand; Data Analytics, the collection, validation, processing, and interpretation of data to obtain useful information and security; Relational Databases, enabling the organization and search of information based on defined relationships; Distributed Data Processing, in which computational tasks can be performed by multiple networked computing systems; and the Internet of Things (IoT), which is a network of inter

$$R(t) = \sum_{i=1}^{n} FI_i(t) * \tau_{ih} + [\tau_h * r_{i-1}] \quad \text{Eq (5)}$$

$$\mathrm{R}^2 = 1 - \frac{\sum_{i=1}^{n}(Y_i - \hat{Y}_i)^2}{\sum_{i=1}^{n}(Y_1 - \bar{Y})^2} \quad \text{Eq (6)}$$

Electronic Health Records (EHRs) and Personal Health Information (PHI) in Health Security and Privacy

One of the most sensitive kinds of information is healthcare data, including personal, financial, and medical data. Its exposure may also cause identity theft, fraud, and massive privacy invasion, and hence, represents an excellent target of cyberattacks and unauthorized access [25, 26]. Bad access controls, misconfigured systems, or specific attacks against electronic health records (EHRs), in addition to exposing personal health information (PHI), tend to damage patient trust and cost organizations significant financial fines [26]. Moreover, there has been an increased number of ransomware incidents where hackers have compromised important systems or data and are holding them for a fee to restore their functionality, causing a critical imbalance in the system as medical services are delayed and lives are endangered [27, 28].

$$\mathrm{RMSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(Y_i - \hat{Y}_i)^2} \quad \text{Eq (7)}$$

Another source of complexity is insider threats, in which employees or contractors accidentally or deliberately share sensitive information [29]. These incidents are very serious and whether it is caused by unauthorized access, negligence or malicious intent, the need to control them without interfering with the privacy of employees or disrupting their work processes is a challenge [30, 31]. The high pace of implementing the Internet of Things (IoT) in healthcare only increases vulnerabilities [32]. Wearable health trackers and other smart medical devices are used to gather and send large volumes of data, but most of them do not have a solid security system, which can easily be hacked or accessed by unauthorized individuals [33]. Although cloud computing improves accessibility and scalability of data, it poses risks like improperly configured data storage, poor encryption, and use of vendors [34]. The need to secure cloud use requires cooperation between healthcare providers and service vendors, which results in accountability gaps [35, 36]. Moreover, adherence to intricate regulatory systems, including the HIPAA in the United States, the GDPR in the European Union, or similar regulations in other countries, may remain indispensable and resource-heavy, and may be quite problematic in small organizations [37, 38].

$$\mathrm{TDI} = \sqrt{(\Delta \mathrm{C})^2 + (\Delta \sigma)^2} \quad \text{Eq (8)}$$

$$\mathrm{MCC} = \frac{\mathrm{TP} * \mathrm{TN} - \mathrm{FP} * \mathrm{FN})}{\sqrt{((\mathrm{TP} + \mathrm{FP}) * (\mathrm{TP} + \mathrm{FN}) * (\mathrm{TN} + \mathrm{FP}) * (\mathrm{TN} + \mathrm{FN}))}} \quad \text{Eq (9)}$$

The use of conventional security programs such as firewalls and antivirus software is not always effective in today's dynamic environment of Internet security threats [39]. Healthcare organizations need to embrace dynamic and proactive approaches to security as threat actors develop more sophisticated approaches. In addition to technical and regulatory issues, there is an even deeper moral aspect of improper handling of sensitive health information. Any disruption of trust and breach of patient consent may negatively affect trust in health systems [40]. In addition, finding the

balance between the necessity to warrant data-driven innovation in the sphere of research, analytics, and AI and the need to ensure privacy is a significant ethical issue that requires strong and progressive solutions to the problem of security [41, 42].

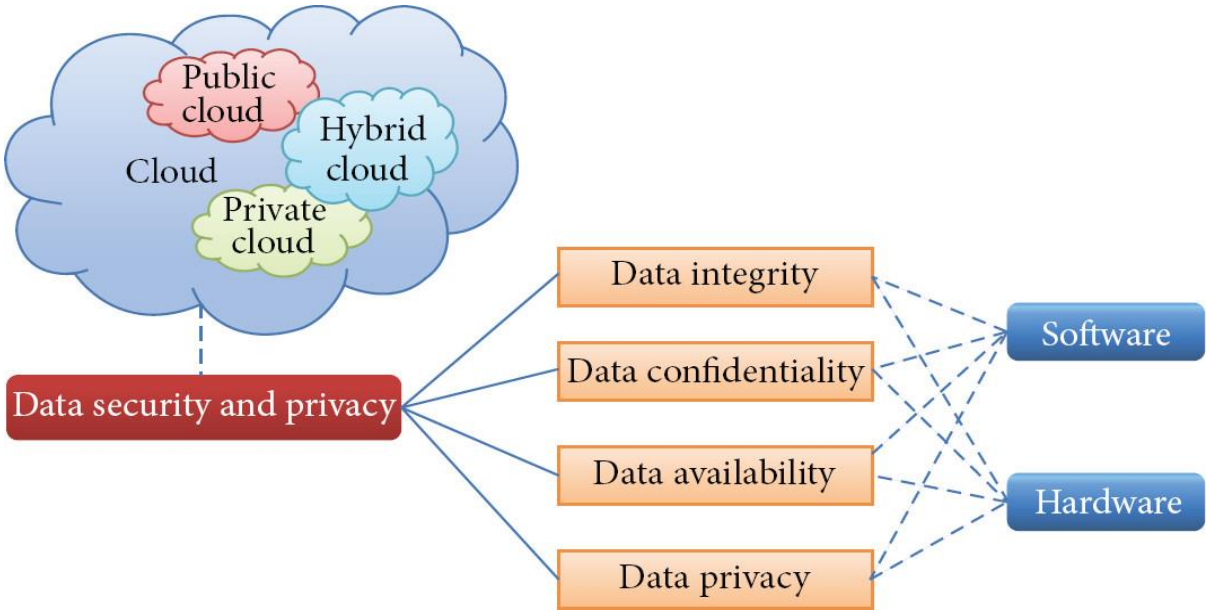

Figure 2.
Challenges in Security and Privacy in Big Data Clouds [43]

Figure 2 above is a visual overview of Challenges in Security and Privacy in Big Data Clouds, which presents the main problems in the area of healthcare data security. This is accompanied by a shield icon, which represents protection in the middle and eight linked boxes outlining a number of challenges. These are data breaches, an emphasis on the exposure of personal health information (PHI) owing to improper system setups and ineffective control access; ransomware attacks, which cripple medical services with lockout of key systems; and insider threats, emphasizing the risks posed by employees or contractors through carelessness or intentional actions [44, 45].

$$Y(t) = \omega[\tau_{ho} * h(t)] \qquad \text{Eq (10)}$$

Big Data in the Health Insurance Portability and Accountability (HIPAA)

The infographic also covers the vulnerabilities of the Internet of Things (IoT), highlighting the security issue in devices such as health monitors and smart medical devices because of poor protocols [46, 47]. Examples of risks associated with cloud computing are provided, highlighting such problems as incorrectly configured storage and reliance on third-party vendors. The difficulties of regulatory compliance highlight how difficult it is to comply with frameworks such as HIPAA and GDPR, especially when the organization is very small. Conventional security restrictions point to the insufficiency of security-by-objective components such as firewalls to threats that are dynamic and ethical consequences emphasize the necessity to have a balance between data-driven innovation and privacy and preserve trust in the community. These components are interrelated and there are arrows between them showing how complex it is to treat the subject of healthcare security holistically [48, 49].

$$\omega = E_f * \frac{1}{1 + e^{-\theta t_f}} \qquad \text{Eq (11)}$$

The Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) are two important legal acts aimed at safeguarding sensitive information, but they have different purposes and goals. HIPAA, which was passed in 1996, is in the healthcare industry of the United States and it only addresses the protection of Protected Health Information (PHI) [50, 51]. It incorporates the Privacy Rule, the Security Rule, the Breach Notification Rule, and the Enforcement Rule [52]. Table 1 demonstrates Global Health Data Region Wise since HIPAA mainly covers data of healthcare providers, health insurance companies, clearinghouses, and the business partners of these companies [53, 54].

Table.1.
Global Health Data Region Wise

Technology Maturity	Regulatory Environment	Key Strengths	Key Challenges	Ref
Highly advanced adoption of EHRs, analytics, AI, and digital health systems	Moderately strong regulations, but enforcement gaps exist	Innovation leadership, strong digital infrastructure, extensive data-driven healthcare initiatives	Frequent data breaches, cybersecurity vulnerabilities, inconsistent policy implementation	[55]
Mature digital health ecosystem with standardized systems in many countries	Very strong; GDPR ensures strict data protection and privacy	High public trust, clear data governance, strong focus on patient rights	Compliance requirements slow down technology adoption; high administrative burden	[56]
Rapid expansion of mobile health apps, telemedicine, IoT health devices	Developing regulatory frameworks; varies widely by country	Fast-growing digital health market, large populations	Lack of interoperability, inconsistent standards, fragmented policies	[57]
Diverse levels: some regions investing in smart health, others still building basic IT capacity	Emerging or evolving regulatory structures	Increased adoption of emerging technologies in advanced economies (e.g., UAE, KSA)	Limited infrastructure, resource constraints, workforce gaps, uneven digital maturity	[58]
Increasing reliance on cloud systems, AI, and global research networks	Lacks unified global framework	Supports global research, pandemic response, and medical tourism	Legal conflicts, privacy concerns, lack of harmonized standards, trust deficits	[59]

GDPR regulates any form of personal information and focuses on the rights of individual privacy [60]. Among the main provisions one may note Data Protection Principles that are concerned with lawful, fair, and transparent data handling; Consent, which requires an informed and freely given consent to use data; Data Subject Rights, which guarantee individuals such rights as access, correction, erasure (right to be forgotten), and data portability; and the rigid Data Breach Notification that obliges to report about a breach to supervisory authorities within 72 hours. GDPR provides a penalty of no less than 20 million euros or 4% of the annual world turnover, whichever is greater, on non-compliance [61, 62]. The two systems vary by a wide margin over the areas of focus, regulatory focus, punishments and personal rights. HIPAA only affects the health information in the United States and is concerned with the compliance of the healthcare sector, but GDPR covers all personal data

concerning the residents of the EU and encompasses all industries [63]. The fines and the rights granted to individuals concerning their data are also much greater under GDPR than in HIPAA. Combined, these structures highlight the significance of strong data protection within their respective areas [64].

LITERATURE REVIEW

With recent shifts towards digital and digital-based healthcare organizations are becoming high-value targets of cybercriminals, nation-state actors, and even malicious insiders. The value of the healthcare data, which includes not only the personal identification information but also the medical history, insurance records, genomic, and financial data, makes them more profitable in the black market than other types of data, including credit card numbers [65, 66]. The healthcare threat environment is dynamic. Data breaches, in case of which a third party receives access to sensitive information about a patient, are among the most frequent and harmful threats. Such violations may happen because of external intrusions or internal security policy failure. Ransomware attacks have also increased in recent years, where attackers secure critical hospital systems and demand payment to recover access that disrupts patient care, postpones surgeries, and endangers lives as the coefficient in Equations 12 and 13 [67, 68].

$$\omega = \left\{ \begin{array}{ll} 0; & normal \\ 0 < \omega < 0.25; & Mild \\ 0.25 < \omega, 05; & Moderate \\ 0.5 < \omega < 0.75; & Severe \\ 0.75 < \omega < 1; & Proliferative \end{array} \right\} \quad \text{Eq (12)}$$

Figure 3 below represents the percentage of frequency of these threats according to the recent data in the industry. In this figure, as can be seen, there is no threat that is overwhelming. Rather, a combination of several vulnerabilities in the behavior of human beings, the integrity of the devices and the configuration of the system that together compromise the security posture of the healthcare organizations. Figure 3 demonstrates the Life Cycle of Big Data from Collection to Destruction that The only way to manage this multi-faceted threat environment is to have a multi-layered defense model, consistent risk evaluation and strong security governance that specifically addresses the healthcare industry [69].

$$\delta_h = 60^{\circ} \left\{ \begin{array}{l} 0 + \frac{(\beta_g - \beta_b)}{(m_x - m_n)}, ifm_x = \beta_r \\ 2 + \frac{(\beta_b - \beta_r)}{(m_x - m_n)}, ifm_x = \beta_g \\ 4 + \frac{(\beta_r - \beta_g)}{(m_x - m_n)}, ifm_x = \beta_b \end{array} \right. \quad \text{Eq (13)}$$

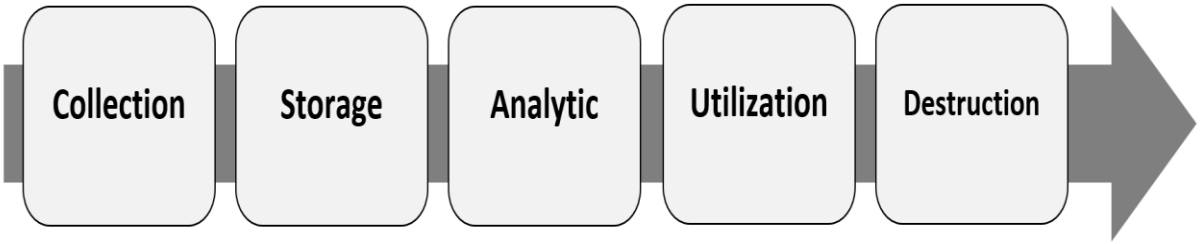

Figure 3.
Life Cycle of Big Data from Collection to Destruction [69]

ACL and Threat Landscape in Big Data

Another threat is insider threats, which are either unintentional or intentional. Data may be abused or mismanaged by employees, contractors, or even third-party vendors who have legitimate access to the systems, and who may or may not cause alerts. This can be very unsafe in places where there is no proper monitoring using role-based access control (RBAC) ACL [70]. The more medical equipment incorporates Internet of Things (IoT) capabilities to include connected insulin pumps, heart monitors, and wearable health trackers, the more entry points there are to attack. Numerous IoT gadgets do not have any built-in security measures and hence can be easily hijacked or their data can be leaked [71, 72].

$$\delta_s = \left(\frac{m_x - m_n}{m_n} \right) \qquad \text{Eq (14)}$$

Cloud misconfigurations also constitute one of the largest vulnerabilities, particularly as healthcare systems move to hybrid and public cloud systems. Badly configured storage buckets, insecure authentication systems, or old versions of software can make whole sets of data available to the internet. In the same vein, the legacy systems that are still prevalent in hospital IT infrastructure and go unpatched leave security blind spots that are hard to track and secure [73, 74]. Various technical and procedural solutions have been implemented within the healthcare industry to curb the increasing threats to healthcare data systems. The following defenses are the basis of the majority of healthcare cybersecurity systems, even though they differ in their effectiveness, scalability, and real-time functionality [75, 76].

$$\delta_v = m_x(\beta_r, \beta_g \beta_b,),\ \delta_{sv} = m_n(\beta_r, \beta_g \beta_b,) \qquad \text{Eq (15)}$$

Threats in Healthcare Data Systems

Encryption, both at rest and in transit, is the key to the protection of healthcare data. Various algorithms such as Advanced Encryption Standard (AES) and Rivest-Shamir Adleman (RSA) are also extensively used to make sure that, in case of unauthorized access, the data will not be read in plain text. Encryption assists in ensuring privacy, particularly when the data is stored in clouds or when it is sent through unsecured networks [77, 78].

$$Y(t) = \omega[\tau_{ho} * h(t)] \qquad \text{Eq (16)}$$

RBAC controls access to data depending on the role and duties of a user, and it is useful in reducing insider threats. More sophisticated designs are being developed,

including Attribute-Based Access Control (ABAC), which offer more fine-grained permissions along with several contextual conditions, such as location, device, or time of access [79, 80]. Scalable data storage is now being done using secure cloud storage platforms, more so the ones that are in compliance with the healthcare regulations (e.g., HIPAA, ISO/IEC 27001). Such services usually include embedded encryption, surveillance and backup services. Nevertheless, the cloud provider and the healthcare organization continue to share the responsibility of security [81, 82].

$$R(t) = \sum_{i=1}^{n} FI_i(t) * \tau_{ih} + [\tau_h * r_{i-1}] \quad \text{Eq (17)}$$

Other techniques are also used to improve privacy and transparency beyond these core technologies. These techniques may assist in minimizing the exposure of data, but can also decrease the utility of data, and may be susceptible to re-identification unless used appropriately [83, 84]. Auditing trails and log systems offer a record of who was able to gain access to what data and when. Most current systems do not have real-time monitoring systems and intrusion detection systems (IDS) that are necessary in detecting and acting on threats as they happen. The major drawback of the existing solutions is that they are reactive. The majority of the technologies are focused on preventing the known threats or responding to an attack, instead of detecting new attack vectors. Also, there is a tendency of performance trade-offs, especially instigated by high security measures on large-scale or real-time systems such as those involved in critical care [85, 86].

$$\omega = E_f * \frac{1}{1 + e^{-\theta t_f}} \quad \text{Eq (18)}$$

$$J_i^{(b,t)} = \beta^{(b)}(S_i^{(b,t)}) \quad \text{Eq (19)}$$

To sum up, though the process of ensuring the safety of healthcare data has been improved considerably, the existing systems should be further adjusted to suit the needs of contemporary, distributed, and smart healthcare ecosystems [87, 88]. Since current security models are having trouble keeping up with the complexity and size of healthcare data landscapes, new technologies are providing some of the most promising paths to patient information security [89, 90]. In addition to improving the security of data, these innovations are also allowing healthcare organizations to use sensitive data more responsibly and ethically [91, 92].

$$J^{(b,t)} = \beta^{(b)} \times (W^{(b)} \times J^{(b-1,t)} + W^{(b)} \times J^{(b,t-1)}) \quad \text{Eq (20)}$$

Blockchain is one of the most disruptive technologies in this field. Initially used in financial operations, blockchain is being modified for healthcare since it can offer audit trails that cannot be compromised, decentralized management, and improved data integrity. In a blockchain, every transaction or access event is logged in a distributed ledger that is not mutable and spread among a number of nodes [93, 94]. To illustrate, access to electronic health records (EHRs) can be monitored with the help of blockchain, which will provide transparency and accountability in the use of data [95, 96].

$$S_i^{(b,t)} = \sum_{z=1}^{E} p_{iz}^{(b)} J_z^{(b-1,t)} + \sum_{i'}^{y} x_{ii'}^{(b)} J_{i'}^{(b,t-1)}$$ Eq (21)

Federated learning Contrary to the conventional machine learning technique, which necessitates the centralization of data, federated learning allows the training of a model by cooperating with a number of institutions without sharing actual patient data. All the participating organizations are trained on the model locally on local data, with only model updates (and not data) being shared with a central aggregator [97, 98]. This would maintain patient privacy; it would also contribute to the construction of robust generalizable models in different populations and care environments [99]. Figure 4 indicates the present adoption rates of these technologies in different areas of healthcare, which reflects the increased interest and the initial applications. Although most of them remain in pilot or initial deployment phases, they demonstrate one of the most important changes toward much more secure and privacy-conscious healthcare systems [104].

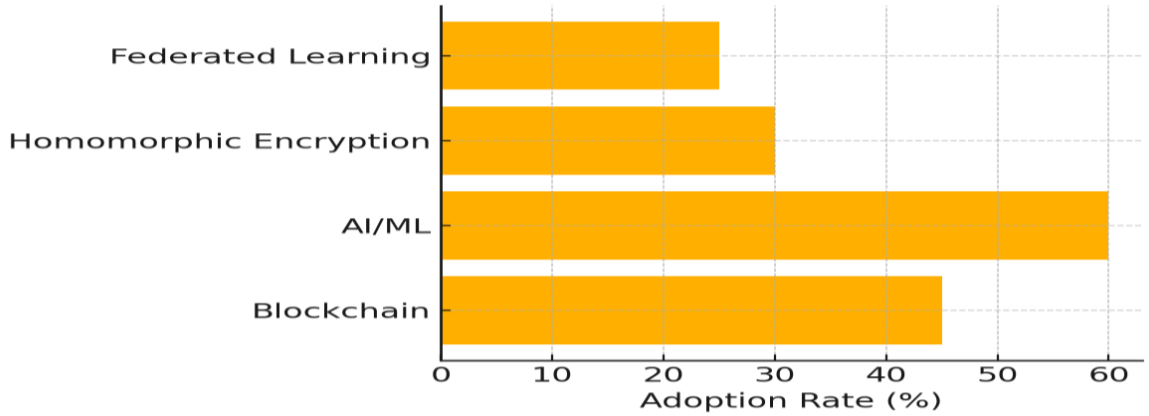

Figure 4.
Adoption rates of emerging security technologies in healthcare.

Encryption enables mathematical functions to be operated directly on encrypted data, producing results, on decryption, are equivalent to those produced in executing the same functions on the plaintext [100]. This implies that healthcare sensitive information can be analyzed, queried, or processed encrypted without having to unveil it in the first place, which fits well in cloud-based analytics or outsourcing computing environments [101, 102]. Secure multiparty computation (SMPC), differential privacy, and zero-knowledge proofs are other newer directions that provide diverse advantages to the privacy and security environment [103].

Remote Sensing Regulatory and Ethical Frameworks

Healthcare data management is regulated by legal and ethical codes of conduct that are developed to safeguard the privacy of patients and promote the responsible utilization of data. The most important law is the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union [105, 106].

$$\ln fl_{it}^{+} = \sum_{j=0}^{t} \Delta \ln W^{T} x + \quad b_{it}^{+} = \sum_{j=0}^{t} \max(\Delta W^{T}{}_{ij,0}) + \epsilon_{it}$$

Eq (22)

HIPAA provides some very transparent guidelines on the protection of Protected Health Information (PHI), defining the manner in which medical organizations are required to store, retrieve, and distribute sensitive information. Instead, GDPR is more comprehensive as it provides people with a wide range of control over their personal data, including the right to access, modify, or demand deletion of their information [107].

$$\ln fl_{it}^{+} = \sum_{j=1}^{t} \Delta \ln W^{T} x + \quad b_{it}^{+} = \sum_{j=1}^{t} \max(\Delta W^{T}{}_{ij,1}) + \epsilon_{it}$$

Eq (23)

Along with the legal considerations, certain ethical principles should be taken into account, including the use of patient information without misusing it, treating the data as the basis of fair and unbiased decisions, and preserving the trust between the patient and the medical professional [108]. Ethical compliance is closely related to legal compliance and supports the idea of responsible data stewardship in the current healthcare system. The practice of healthcare data is also largely differentiated by region and is affected by the maturity of the technology involved, regulatory establishments, and healthcare priorities. Data-driven healthcare system is one of the best developed in North America, where the extensive use of electronic health records, analytics platforms, and AI-based tools is present [109, 110].

$$B_{m,n}(q+1)\left(1 - \frac{1 - X(0,1) - X(-1,1)}{1 - c_{m,n} \times f_{mn}(q)}\right) = X(0,1) \times R_{s,n}$$

Eq (24)

Nevertheless, the area is still characterized by high-profile data breaches, and it serves to demonstrate that there are still vulnerabilities in policy enforcement and cybersecurity preparedness. In Europe, patient privacy is the focal point of digital health efforts due to strong regulatory frameworks, especially the GDPR [111, 112].

Such a rigid compliance culture has contributed to the development of community trust, although the system has the tendency to delay the integration of new technologies as a result of high demands. In Asia, other countries like China and India are also experiencing a booming mobile health applications, telemedicine and digital health infrastructure [113, 114].

$$E_c = \frac{1}{K} \times \sum_{g=1}^{k} J_v^{b,t} - k_v$$

Eq (25)

Whereas countries are putting major investment in the development of smart health systems and new technologies, countries are grappling with the basic challenges of infrastructure, workforce capacity, and resources [115]. Cross-border health data sharing is emerging as a national challenge in the world, especially as patients become mobile, as research goes international, and as a pandemic demands concerted efforts. To attain safe and ethical international data exchange, there is a

need to have harmonized policies, common standards, and mutual trust between the nations [116, 117].

$$\ln fl_{it}^{+} = \Sigma_{j=2}^{t} \Delta \ln W^{T} x + \quad b_{it}^{+} = \Sigma_{j=2}^{t} \max(\Delta W^{T}{}_{ij,2}) + \epsilon_{it} \quad \text{Eq (26)}$$

Despite the fact that the security of healthcare data has been improved greatly, there are still a number of gaps that are of high importance. To illustrate, although blockchain and federated learning have been extensively covered in scholarly literature, their practical use in large-scale healthcare settings is yet to be validated. The available studies mostly use small datasets or simulation conditions and their relevance to real-life situations is limited. The other significant interoperability gap is in interoperability. Many healthcare providers in various countries and even within the same region are still grappling with the issue of interoperability of various Electronic Health Records (EHRs) [118, 119]. The absence of a smooth exchange of data slows down the process of care delivery and makes cross-border health partnerships more difficult. Likewise, the application of AI-based threat detection in real-time is not established in the healthcare production systems. Most hospitals use traditional security equipment and lack the benefits of the advanced anomaly detection that will allow them to potentially detect attacks or abnormal data patterns in advance [120, 121].

$$\ln fl_{it}^{+} = \Sigma_{j=2}^{t} \Delta \ln W^{T} x + \quad b_{it}^{+} = \Sigma_{j=2}^{t} \max(\Delta W^{T}{}_{ij,2}) + \epsilon_{it} \quad \text{Eq (27)}$$

Research Gaps

Lastly, the area does not have established standards to measure the efficiency of security solutions. The aforementioned research gaps need to be addressed in the future by more pragmatic, high-scale, and standardized research to solidify the security and resiliency of healthcare big data ecosystems [122, 123]. Automated protection using smart-intelligent protection devices will become the main means of securing healthcare data. Artificial intelligence-based security orchestration and zero-trust schemes will be at the center of securing the fact that all access requests to a network, either by a user, device, or application, are constantly verified. With the increased use of AI in the clinical decision-making process, the Explainable AI (XAI) will become increasingly important, and healthcare providers will know why an algorithm has given a particular recommendation [124, 125].

The ongoing convergence of the IoT devices, big data analytics, and genomic data will form giant rivers of sensitive data, compelling organisations to embrace a hybrid architecture with the capability to offer both stringent privacy regulation as well as high-performance processing. We can also expect the emergence of common interoperability standards and even global cybersecurity agreements to facilitate the sharing of medical information across countries without complications and risks [126, 127].

All these trends are pointing to the future of more intelligent, transparent, and globalized healthcare security ecosystems. This paper analyzed the multifaceted nature of big data security in healthcare, illuminating the most significant challenges, the current defense measures, and the new technologies that define the future [128].

Table 2.

Category	Description / Key Points	Impact on Healthcare Data Security	Ref
Global Significance	• Healthcare data is critical and highly sensitive • Cross-border research and telehealth increase exposure risks • Worldwide shift toward digital health ecosystems	Elevates the need for unified, global efforts in securing medical data	[129]
Future Strategy Requirements	• Integration of strong technical safeguards • Consistent regulatory compliance across regions • Ethical and responsible data governance	Supports the development of secure, trustworthy, and equitable healthcare technologies	[130]
Desired Outcome	• Secure innovation without compromising privacy • Trustworthy digital healthcare systems • Equitable access to safe big data technologies	Ensures long-term sustainability and public confidence in data-driven healthcare	[131]
Primary Challenges	• Increasing data volume and sensitivity • Cybersecurity threats and breaches	Creates vulnerabilities across healthcare systems and highlights the need for stronger, adaptive security measures	[132]
Existing Protective Mechanisms	• Advanced encryption methods • Access control and authentication systems • Network security tools (firewalls, IDS/IPS) • Compliance frameworks (HIPAA, GDPR)	Builds foundational security, mitigates known threats, and ensures adherence to legal requirements	[133]
Emerging Technologies	• Federated learning for privacy-preserving analytics • AI/ML-based anomaly detection • Zero-trust security architectures	Introduces innovative, scalable solutions to address modern data challenges and enhance protection	[134]

Regardless of using sophisticated encryption, blockchain-based mechanisms, or privacy-saving architectures, it remains evident that data protection in healthcare is a continuous and globally important task. It is through harmonizing these factors that the healthcare sector can be able to guarantee that innovation progresses in a safe, credible and fair manner [135].

METHOD AND MATERIALS

Healthcare big data offers transformative benefits, but its adoption is constrained by serious security and privacy concerns:

- Risks during data collection, transmission, storage, and usage
- Fragmented data governance and weak interoperability
- Vulnerability of IoT and cloud systems to cyber threats

Balancing usability and privacy under strict regulations (HIPAA, GDPR) ways that healthcare organizations can deploy a scalable, hybrid model to guarantee the sound security, privacy, and usability of medical big data without violating international standards. Having provided the description of the concept of medical

big data, the security and privacy issues and their protection measures, the main task of this section is to underline the fact that our innovative access control model will help to improve the security and privacy of medical big data. Overall, access control is used to establish the identity of the user and restrict unauthorized users to the access to the resources. According to it, we intended to build a new access control model that will not allow unauthorized users to access the medical big data stored in the cloud environment through the implementation of the Access control model.

Data Collection and Analysis

As part of the methodology, the data is used on both primary and secondary levels, where the Primary Data will be Review of hospital ICT infrastructure, IoT-enabled devices, PACS/EHR integration and Simulation of data flow in hybrid cloud environments and the Secondary Data will be based on Literature by IEEE, Springer, Elsevier (post-2020). Blockchain-based healthcare and secure IoT networks case studies. The Analysis Technique is founded on Threat modeling (STRIDE, CVSS). Statistical validation, SmartPLS or similar. Data transfer simulation by means of an Access control ACL scheme.

Proposed Efficient Framework for Preserving Big Data Analytics in Cloud

The access control system is used in our proposed Efficient Model of Preserving Big Data Analytics in Cloud. It is constructed based on a few fundamental elements, with them being the public cloud, the private cloud, the data owners, the management of authority, the administrative authority, super/override users and the end users. All these have their unique functions in ensuring and controlling access to the system. The major data storage location is the public cloud, where massive amounts of medical data are stored. This encompasses diagnostic outcomes, imaging, and other health records that are made with the help of different medical equipment. This is a cloud infrastructure that is deployed on a platform like Amazon Web Services (AWS) or Microsoft Azure, which is not directly under the control of the healthcare organization. Consequently, the information on the public cloud is encrypted to promote privacy and discourage unauthorized access. Both end users and data owners (e.g., physicians, radiologists) are allowed to interact with the public cloud, but are strictly controlled with permissions granted by the system.

The solution combines the hybrid cloud storage + hierarchical RBAC + hybrid encryption (ACL). After a thorough examination of available literature and access control models, we determined the merits and demerits of different strategies applied in healthcare data protection. Based on the deliberation, we decided to use a hierarchical Role-Based Access Control (RBAC) model in our proposed architecture. The model offers the finer-grained control of access that is necessary to make sure that the sensitive medical information is seen only by the necessary people, and at the same time to be able to scale and be flexible enough to keep up with the real-life medical environment. The difference between our approach and the past models is that we have combined a hybrid cloud architecture with the ability to deploy both public and private cloud infrastructure in addition to hybrid cryptographic scheme which involves the use of both AES (128-bit) and RSA (1024-bit) algorithms.

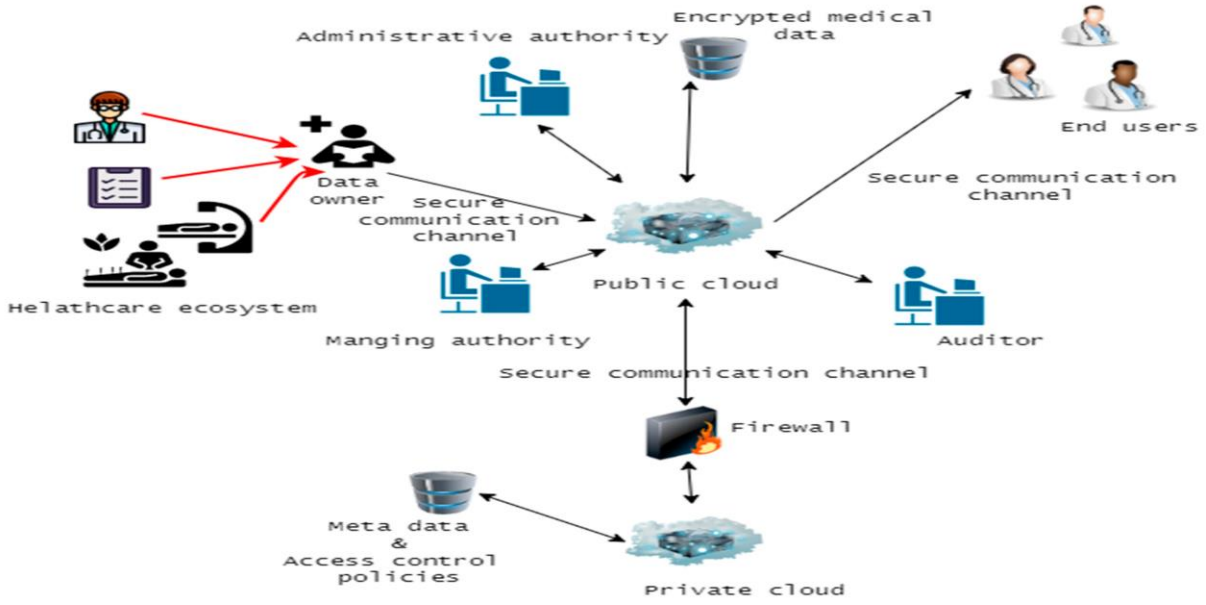

Figure 5.
Proposed Model for Preserving Big Data in Cloud-based on ACL

Particularly, we apply the AES algorithm to encrypt and decrypt large amounts of medical big data on the public cloud, and RSA encryption to protect the AES generated secret keys and related metadata. This hierarchical cryptographic design provides a formidable degree of security to the information as well as the keys used to de-encrypt it.

Administrative Authority and Secure Big data sharing and attack detection framework

The private cloud is a secure internal data center that is found within the healthcare organization. It holds sensitive information, metadata of operations including encryption keys, access control policy and user credentials. This cloud is controlled by the organization itself, which in turn provides a better chance to control the security measures and deploy firewalls, honeypots, and other defensive tools. The amount of data being processed in the private cloud is significantly less than that in the public cloud, hence the lower computation and operating overheads. The integration provides a valuable addition of protection to the entire architecture.

The architecture is an administrative authority, which is an internal entity tasked with the role of access control to the system at a high level. It can issue authorizations and grant role managers and end users to do certain things. When the situation is critical, the administrative authority may assign some users as an override or super user, who have complete access to the encrypted data, where necessary. This position makes sure that exceptions needed can be achieved without affecting the overall system security. The managing authority has the responsibility to manage role management and the user role relationship in the system. It establishes roles as per the organizational requirements, roles, and level of access.

It also adheres to the principle of least privilege, which states that users are only granted the bare minimum of permissions that are necessary to carry out their tasks. The managing authority is also able to add new positions or expand on the existing positions by inheriting features of the positions above them and this increases the

flexibility of the RBAC structure. It is also authorized to cancel user access and limit the creation of temporary or ad-hoc roles as required.

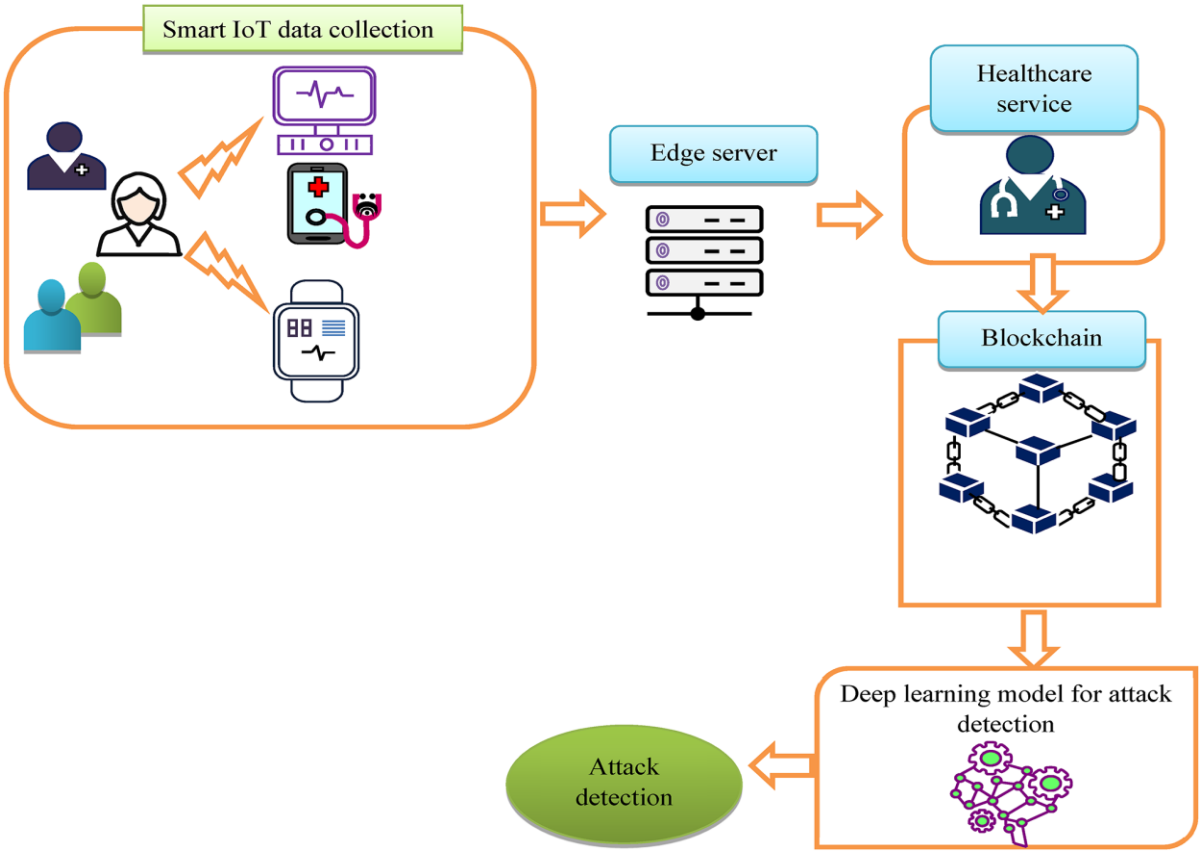

Figure 6.
An Enhanced Architecture for Secure Big data sharing and attack detection framework

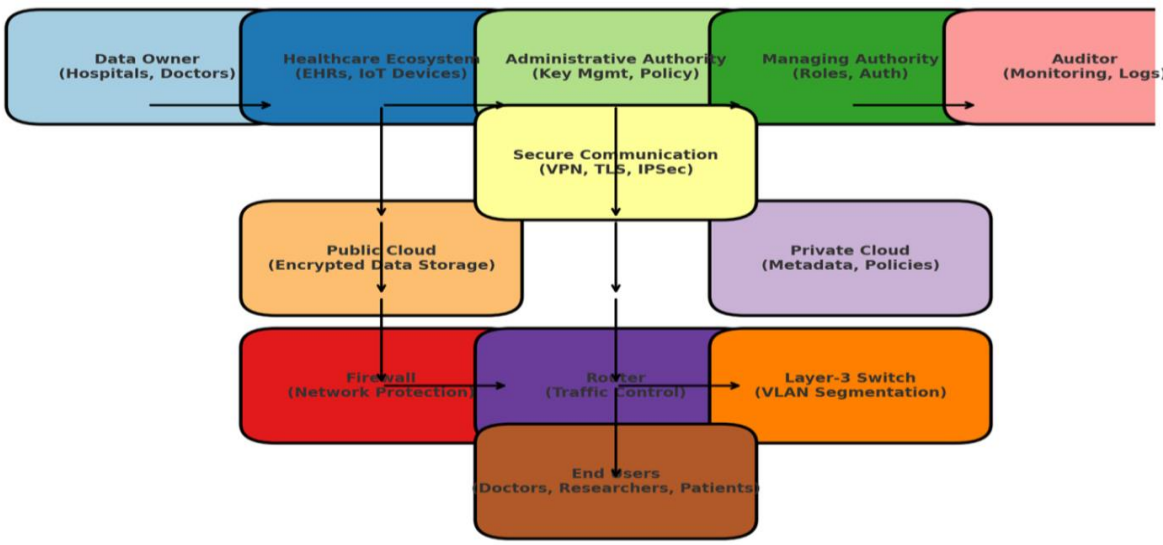

Figure 7.
Block Diagram schema of Proposed Model

It is a security model that is proposed to have a multi-layered security approach to managing medical big data within a healthcare setting. The system will be able to

secure the medical data at all levels by using hierarchical RBAC, a hybrid cloud system, and strong encryption services to protect the medical data in the generation and storage phases, as well as in the process of retrieving and sharing information without compromising the usability for the authorized stakeholders. End user: Every authorized customer, internal or external, desires to access the data stored in the cloud. • Auditor An auditor will monitor system transactions, user behaviors, and other unusual occurrences in the system. Giving users override in some situations, users in an organization may require quick access to data when there is an emergency. The administrative authority can, therefore, create parameters of the users of the override and enter them into the system within a real-time framework and the override user can later have full access to stored big data.

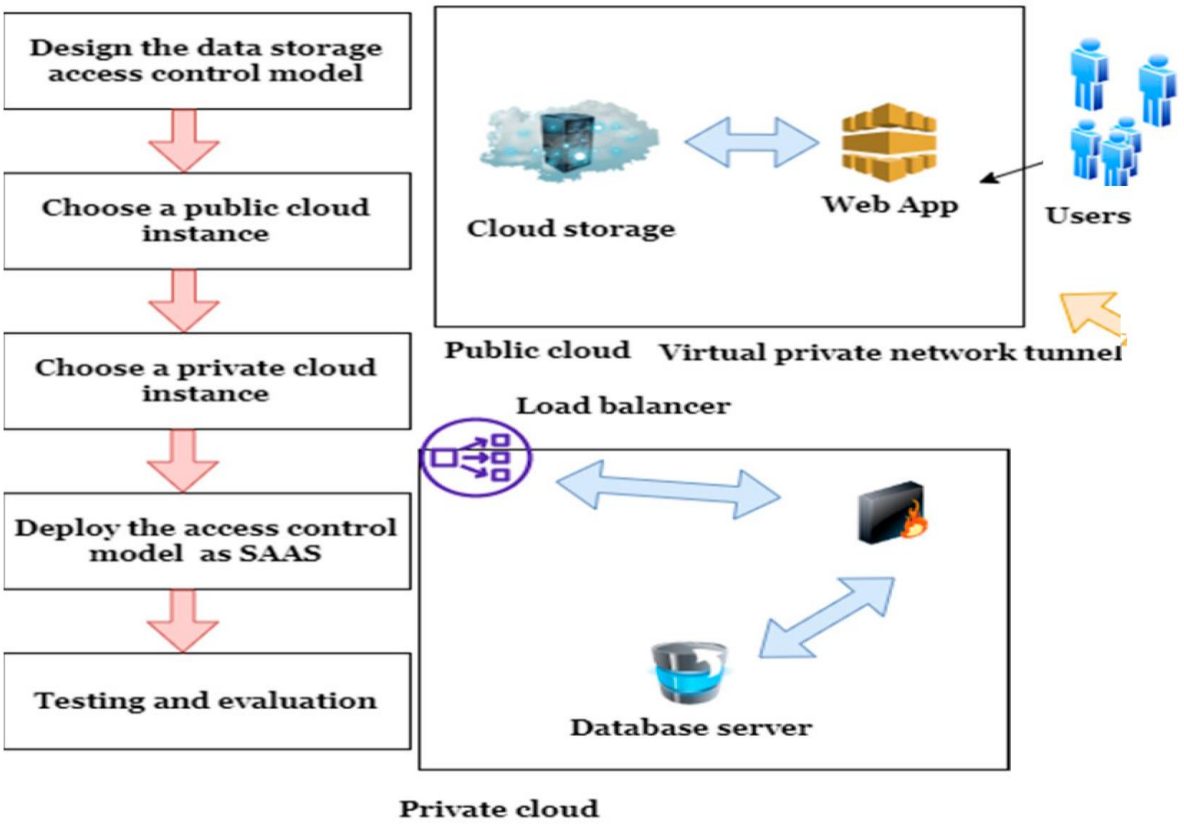

Figure 8.
Step by step Flow of Proposed Access Control Model

The above Figure 8 shows by step Flow of the Proposed Access Control Model that shows storage to testing evaluation and the users as participants of the healthcare organization, i.e., doctors, lab technicians, or other medical personnel, are expected to gather and upload data to the public cloud. In addition to uploading data, data owners are also important in shaping data access control and role definitions that only users who have permission to access the encrypted information can access the information. This assists in implementing granular access control at the creation of the data. The wider category of stakeholders that need access to the medical information stored in the public cloud is known as end users. These may be healthcare workers, insurers, researchers or even caregivers. Although the end users can view and access data, they cannot make changes or communicate directly communication to the infrastructures of the private cloud. The roles and the permissions assigned by the administrative and the managing authorities control their access, and all the actions are safe, traceable, and supervised by the role.

Implementation of the Proposed Model

Step 1**:** Encrypt Patient Records Locally (AES-128)

- **Process:** Before any medical record leaves the hospital, it is encrypted using the Advanced Encryption Standard (AES-128)**.** This is a symmetric key algorithm, meaning the same key is used for both encryption and decryption.

- **Rationale:** Encrypting data at the source ensures that even if attackers intercept the file during transmission, they cannot read or manipulate it without the key. AES-128 is fast, lightweight, and suitable for large volumes of medical data such as images, test results, and EHRs.

- **Outcome:** Patient records remain confidential and protected before leaving the secure hospital environment.

Step 2: Upload Encrypted Data to Public Cloud

- **Process:** The AES-encrypted data is transferred to a public cloud infrastructure (e.g., AWS, Azure, or Google Cloud).

- **Rationale:** Public clouds are scalable and cost-effective, capable of handling petabytes of medical records and supporting real-time access across geographies.

Outcome: Encrypted data becomes accessible to authorized users remotely, while the raw unencrypted patient data never leaves the hospital's secure environment.

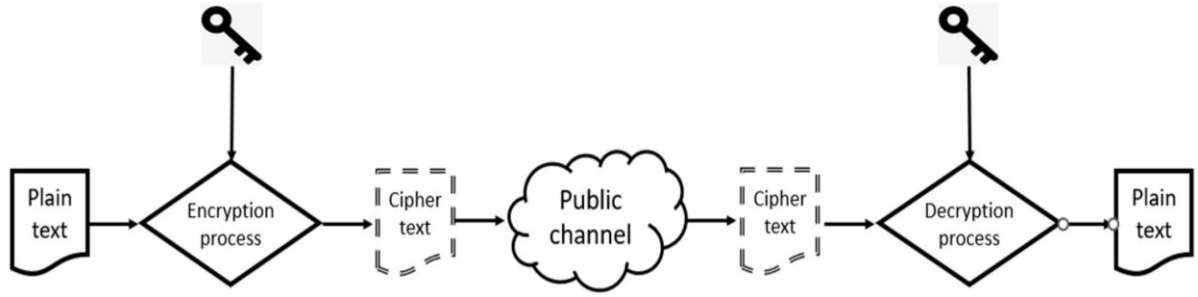

Figure 9.
Healthcare Data security flow step by step following encrypted channels

Evaluation Metrics

A detailed side comparison is employed in this section to compare the proposed Network Security and Privacy Model that has been integrated with Virtual Private Network (VPN) and Virtual Local Area Network (VLAN) and the Current Simplified Architecture that is currently in use. This comparison is made to have a clear understanding of the differences in the design philosophy, safeguards in operation and resilience against contemporary cybersecurity threats.

In order to provide a balanced evaluation, the assessment will cover nine key areas of security and privacy, such as network segmentation, user access control, firewall configuration, intrusion detection, encryption standards, backup resiliency, threat response procedures, privacy compliance, and scalability. The rating of each aspect is based on a numerical scale between 1 (lowest) and 5 (highest) and, therefore, the analysis can integrate quantitative scoring with qualitative observations. This two-lens design does not only reflect the technical performance of the model but also demonstrates the real-life use of the model in a health facility.

Comparative Analysis of Security and Privacy Models

Table 3.
Comparative Analysis of Big data based security in healthcare Proposed Model and Current Model

Feature	Proposed Model (with VPN & VLAN - More Detailed)	Current Model (Simplified Architecture)	Comparison Summary
Network Segmentation	Introduces a Layer-3 VLAN switch and router, enhancing segmentation and isolation of internal users.	No VLAN or router shown; assumes a flat network structure.	Proposed Model is more secure due to network segmentation, reducing internal threat exposure.
User Access Control	Differentiates between inside users and outside trusted users (VPN). Uses role-based access via managing authority.	All users appear as generic end users; lacks segmentation between internal/external.	Proposed Model enhances privacy by clearly limiting external access through VPN.
Firewall Usage	Explicitly shows a firewall between public and private cloud, enforcing stricter security policies.	Firewall present but not contextually enforced between user roles or data layers.	Proposed Model for better control and threat mitigation via layered protection.
Communication Channels	All communication is marked as secure, implying encryption protocols in transit (TLS/SSL, etc.).	Also shows secure channels, but lacks detail for endpoint controls and traffic filtering.	Both are comparable, but Proposed Model implies stricter enforcement.
Cloud Usage (Hybrid)	Shows public cloud for encrypted medical data and private cloud for metadata and access control policies.	Similar structure, but lacks detail on cloud communication pathways and hierarchy.	Proposed Model provides clarity in enforcing least privilege and data separation.
Role Hierarchy	Strong visual presence of managing authority and administrative authority with well-defined roles.	Similar structure but less emphasis on dynamic role management or revocation policies.	Proposed Model promotes better accountability and real-time access policy control.
Data Ownership & Upload	Data owner is central, directly linked to healthcare ecosystem and cloud upload.	Same data owner role, but fewer visual cues for accountability chain.	Comparable, though Proposed Model offers a better trace of data flow origins.
Audit Trail & Compliance	Includes auditor role, indicating periodic reviews and log verification.	Auditor also present, but Diagram A suggests closer integration with security flow.	Proposed Model better supports compliance needs like HIPAA audits or access tracking.
Threat Surface	Reduced through firewalls, VLANs, VPNs, and split responsibilities.	Broader threat surface due to fewer isolation layers and external access visibility.	Proposed Model is more resilient to insider and outsider threats.

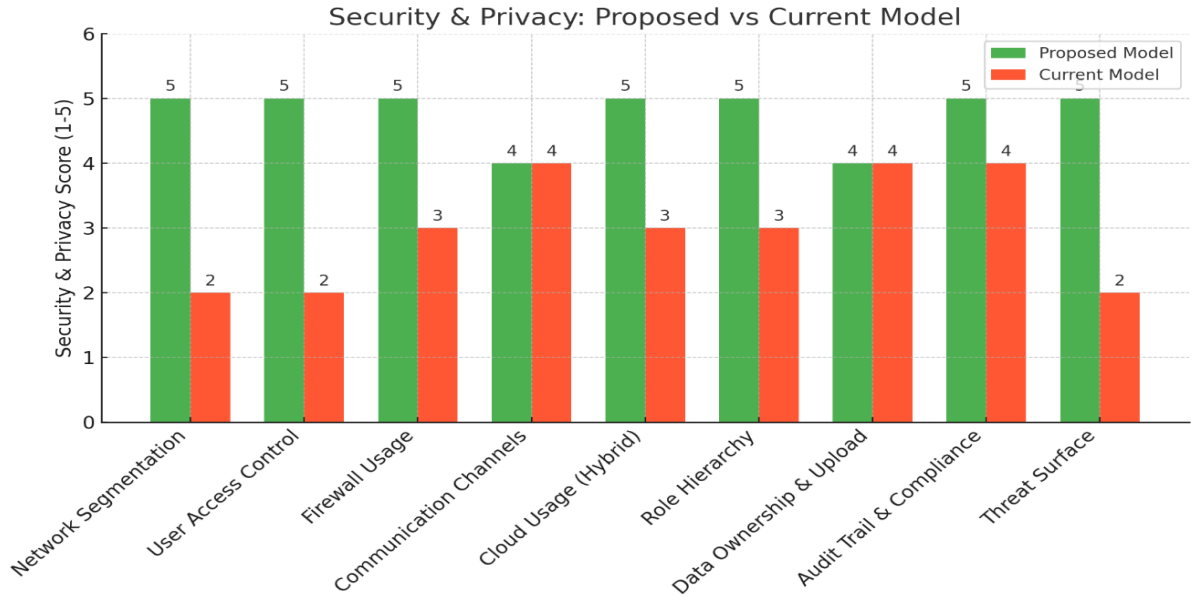

Figure.9.
Security & Privacy Proposed vs Current Model

The Current Model is operationally simple but it works in a highly flattened network topology. This ease of maintenance comes at the cost of opening the critical systems because both internal and external users operate without much segregation. Firewalls and other security controls are applied on a rudimentary level and minimal enforcement of role-based-access or data-layer controls is applied.

On the contrary, the Proposed Model proposes layered defenses in accordance with modern cybersecurity best practices. The VPN technology prevents unauthorized external users and allows only the authenticated ones to have access to the network and the use of the VLAN-based segmentation restricts the possibility of threats spreading further in the network in the future. Other services like deployment of next-generation firewalls, sophisticated encryption protocols, and central access controls are among other services that result in an increased level of security posture and compliance preparedness of the system.

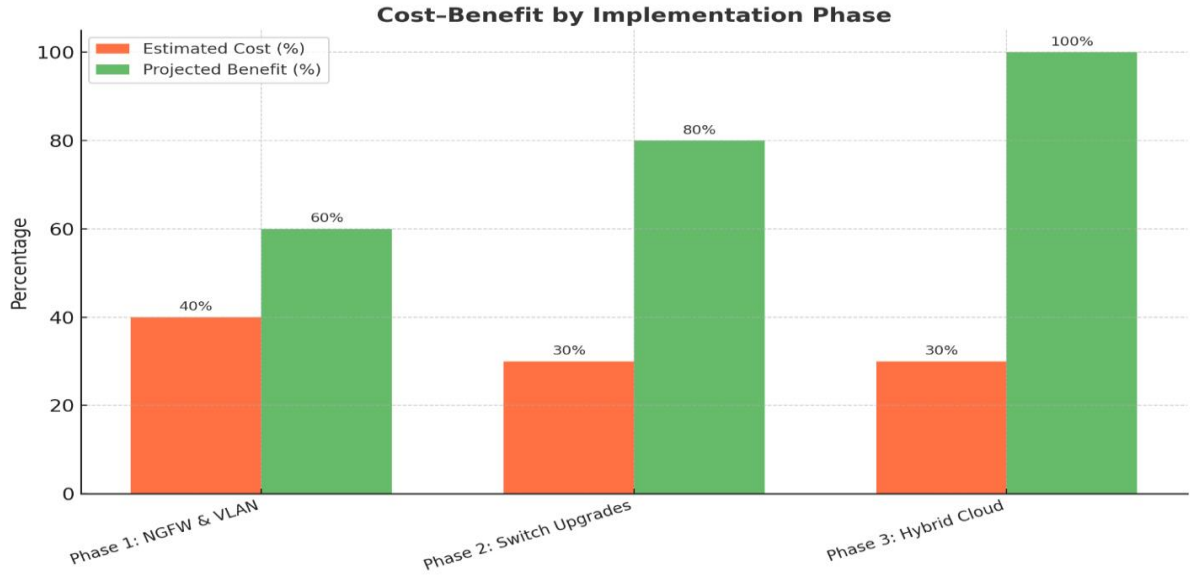

Figure 10.
Cost Benefit of Implementation Phase

Table. 4.
Comparative Analysis of ACL Model in Big data based security

Model	Access is Granted	Access Permissions	Security Implications
DAC	Based on the identity of the user	Permissions are defined on the access control list.	Easily vulnerable to exploit
MAC	Given by the system administrator	The administrator has the full authority to change the security clearance of an object and users.	Vulnerable to exploit
Proposed Model	Based on the role assigned to an end user by the system administrator	Rhe system administrator centrally manages the responsibilities by securing the Network Segmentation, User Access Control And Threat Surface monitoring	More secure and resilient than the MAC and DAC models

Table5.
Analysis of Big data based security in healthcare based on Proposed Model

Model	Feature / Parameters	Improvement (%)	Feature / Parameters	Improvement (%)
Proposed Model	Network Segmentation	1.5%	Cloud Usage (Hybrid)	6.7%
	User Access Control	1.5%	Role Hierarchy	6.5%
	Firewall Usage	6.7%	Data Ownership & Upload	0.45%
	Communication Channels	0.2%	Audit Trail & Compliance	2.5%
	Threat Surface 1	1.5%	Threat Surface 2	1.5%

The above section presents a side-by-side comparison between the Proposed Network Security & Privacy Model (featuring VPN and VLAN integration) and the Current Simplified Architecture. The assessment covers critical aspects of security and privacy, each rated on a scale. The analysis blends qualitative observations with quantitative scoring to provide a balanced view of each model's strengths and weaknesses. Figure below shows the comparative performance of the two models. On average, the Proposed Model scored 4.78% better as compared to the Current Modelss. This difference is not just numerical; it represents a tangible step forward in protecting healthcare data.

CONCLUSION

The potential of using big data to transform healthcare to new heights is real. Nonetheless, some issues like security and privacy are challenging the success of the technology and which should be resolved as soon as possible. The security and privacy implications of medical big data were considered in this research and the necessity of security and privacy preventive measures was also addressed. Moreover, a new cloud-based hybrid access control architecture was suggested, which may be applied in building secure medical big data. As we have reviewed, security and privacy preventive mechanisms are supposed to be part and parcel of the medical big data lifecycle, including the data generation, processing, and storage. The research also summarized the knowledge and suggested that safe patient information management is a critical component of universal healthcare. It presented the new access control model based on medical big data that has been proposed and summarized the related work. In general, the suggested access control model may be applied to organizations both in commercial and non-commercial applications, where access control may be defined based on job functions within the organization. The paper provides a comparative analysis of proposed solutions, taking into account a great number of parameters and reveals important gaps to build more secure and trustworthy healthcare systems. The results indicate that the

model can be applicable in the assessment of the current safety threats and the prediction of the extent of the different risk factors, by showing that Network Segmentation and Cloud Usage (Hybrid) have increased the outcome by 1.5% and 6.7% respectively and the User Access mechanism is improved by 1.5% and 6.7% respectively. The Audit Trail and Compliance are also becoming better because the suggested method will analyze the ACL and investigate the major international regulatory frameworks, such as the GDPR and HIPAA. Thus, the future work can enhance the proposed access control model with a better encryption schema and be empowered with a rigid, efficient authentication schema. The proposed model, on the other hand, can be combined with artificial intelligence-based solutions in designing more resilient, secure access control models on real-time threat detection and prevention. The research outcomes of this paper will lay the foundation on which future researchers will conduct their work in this field, taking the account that security and privacy are the most important aspects of researchers in this domain.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributor to the research and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally in the creation of this work.
Conflicts of Interest: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

A. Ali, M. A. H. Farquad, C. Atheeq, and C. Altaf, "A Quantum Encryption Algorithm based on the Rail Fence Mechanism to Provide Data Integrity", Eng. Technol. Appl. Sci. Res., vol. 14, no. 6, pp. 18818–18823, Dec. 2024.

Abdullah, M. M., Ghafoor, U., Qadeer, Q. B., Khadim, F., Khan, H. S., Ahmad, A., & Khan, H. (2025). An Efficient of Artificial Intelligence based Brain Tumor Diagnosis and Classification: An Advance Medical Diagnosis Approach. The Asian Bulletin of Big Data Management, 5(2), 208-242.

Abdullah, M. M., Ghafoor, U., Qadeer, Q. B., Khadim, F., Khan, H. S., Ahmad, A., & Khan, H. (2025). An Efficient of Artificial Intelligence based Brain Tumor Diagnosis and Classification: An Advance Medical Diagnosis Approach. The Asian Bulletin of Big Data Management, 5(2), 208-242.

Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. Procedia Computer Science, 113, 73-80.

Adadi, Amina, and Mohammed Berrada. "Explainable AI for Healthcare." Artificial Intelligence Review, Springer, 2020.

Adil, M. U., Ali, S., Haider, A., Javed, M. A., & Khan, H. (2024). An Enhanced Analysis of Social Engineering in Cyber Security Research Challenges, Countermeasures: A Survey. The Asian Bulletin of Big Data Management, 4(4), 321-331.

Ahmad, I., Nasim, F., Khawaja, M. F., Naqvi, S. A. A., & Khan, H. (2025). Enhancing IoT Security and Services based on Generative Artificial Intelligence Techniques: A Systematic

Analysis based on Emerging Threats, Challenges and future Directions. Spectrum of engineering sciences, 3(2), 1-25.

Ahmad, J., Salman, W., Amin, M., Ali, Z., & Shokat, S. (2024). A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. Spectrum of Engineering Sciences, 2(4), 133-149.

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An insightful Machine Learning based Privacy-Preserving Technique for Federated Learning. The Asian Bulletin of Big Data Management, 4(4), 332-343.

Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (AI) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power IoT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

Al Zaabi, M., & Alhashmi, S. M. (2024). Big data security and privacy in healthcare: A systematic review and future research directions. Information Development, 02666669241247781.

Ali, A. (2019). Intelligent Auto Traffic Signal Controller for Emergency Vehicle by Using. Journal of Engineering and Applied Sciences, 14(1), 76-82.

Ali, A. (2022). A framework for air pollution monitoring in smart cities by using IoT and smart sensors. Informatica, 46(5).

Almalawi, A., Khan, A. I., Alsolami, F., Abushark, Y. B., & Alfakeeh, A. S. (2023). Managing security of healthcare data for a modern healthcare system. Sensors, 23(7), 3612.

Alsubaei, Faisal, et al. "Security and Privacy in IoT Healthcare: Review." Applied Sciences, MDPI, 2021.

Alzu'bi, Ahmad, et al. "Privacy and Edge Computing in Smart Healthcare." ResearchGate, 2024.

Anas, M., Imtiaz, M. A., Saad Khan, A. A., Naghman, N. F., Khan, H., & Albouq, S. AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING. Vol.-20, No.-3, March (2025) pp 54 - 72

Aqeel, I., et al. "IoT Smart Medical Devices in Healthcare." IEEE Access, 2021.

Aqeel, N., Alam, A., Bhatti, Z., & Amir, A. (2024). A Survey on Tor's Multi Layer Architecture and Web Implications in Dark Web. Spectrum of Engineering Sciences, 2(4), 212-231.

Asghar, M. A., Aslam, A., Bakhet, S., Saleem, M. U., Ahmad, M., Gohar, A., & Khan, H. (2025). An Efficient Integration of Artificial Intelligence-based Mobile Robots in Critical Frames for the Internet of Medical Things (IoMTs) Using (ADP2S) and Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 160-183.

Aslam, I., Tariq, W., Nasim, F., Khan, H., Khawaja, M. F., Ahmad, A., & Nawaz, M. S. (2025). A Robust Hybrid Machine Learning based Implications and Preventions of Social Media Blackmailing and Cyber bullying: A Systematic Approach.

Ayub, N., Alghamdi, T., Din, I., Ali, A., Khan, H., Ganiyeva, O., & Makhmudov, S. (2025). An Enhanced Artificial Intelligence and Deep Learning Assisted Breast Cancer Classification and Diagnosis Based on the Internet of Medical Things (IOMTs). Engineering, Technology & Applied Science Research, 15(6), 30612-30616.

Ayub, N., Alghamdi, T., Din, I., Ali, A., Khan, H., Ganiyeva, O., & Makhmudov, S. (2025). An Enhanced Artificial Intelligence and Deep Learning Assisted Breast Cancer Classification and Diagnosis Based on the Internet of Medical Things (IOMTs). Engineering, Technology & Applied Science Research, 15(6), 30612-30616.

Ayub, N., Anwer, M. A., Iqbal, A., Rizwan, S. M., Shahbaz, A., Abid, M. H., & Rafi, S. (2025). Enhanced ML Framework based on Artificial Neural Network for countermeasures of Data Protection and Network Vulnerabilities Detection in Industrial Internet of Things. Annual Methodological Archive Research Review, 3(5), 410-431.

Aziz, R., Mehmood, A., Tariq, A., Nasim, F., Farooq, U., Naqvi, S. A. A., & Khan, H. (2025). Critical Evaluation of Data Privacy and Security Threats: An Intelligent Federated Learning-based Intrusion Detection System Poisoning Attack and Defense for Cyber-Physical Systems its Issues and Challenges Related to Privacy and Security in IoT. The Asian Bulletin of Big Data Management, 5(1), 73-84.

Bacha, A., Sehar, H., Naseem, S., & Khan, M. I. (2024). FEDERATED LEARNING FOR THREAT

INTELLIGENCE SHARING: A PRIVACY-PRESERVING COLLABORATIVE DEFENSE MODEL. Spectrum of Engineering Sciences, 656-664.

Badr, Yasmine. "The Use of Big Data in Personalized Healthcare." Frontiers in Medicine, 2024.

Criado, M.F.; Casado, F.E.; Iglesias, R.; Regueiro, C.V.; Barro, S. Non-iid data and continual learning processes in federated learning: A long road ahead. Inf. Fusion 2022, 88, 263–280.

Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

Farooq, I., Ahmed, S. A., Ali, A., Warraich, M. A., Aqeel, M., & Khan, H. (2024). Enhanced Classification of Networks Encrypted Traffic: A Conceptual Analysis of Security Assessments, Implementation, Trends and Future Directions. The Asian Bulletin of Big Data Management, 4(4), 500-522.

Farooq, M., Younas, R. M. F., Qureshi, J. N., Haider, A., & Nasim, F. (2025). Cyber security risks in DBMS: Strategies to mitigate data security threats: A systematic review. Spectrum of engineering sciences, 3(1), 268-290.

Fatima, M., Ali, A., Ahmad, M., Nisa, F. U., Khan, H., & Raheem, M. A. U. Enhancing The Resilience Of Iot Networks: Strategies And Measures For Mitigating Ddos Attacks. Cont.& Math. Sci., Vol.-19, No.-10, 129-152, October 2024 https://jmcms.s3.amazonaws.com/wp-content/uploads/2024/10/10072102/jmcms-2410025-ENHANCING-THE-RESILIENCE-OF-IOT-NETWORKS-MF-HK.pdf

Fawy, K. F., Rodriguez-Ortiz, G., Ali, A., Jadeja, Y., Khan, H., Pathak, P. K., ... & Rahman, J. U. (2025). Catalytic exploration metallic and nonmetallic nano-catalysts, properties, role in photoelectrochemistry for sustainable applications. Reviews in Inorganic Chemistry, (0).

Ghafoor, U., Ayub, N., Yaseen, A., Anas, M., Farooq, I., Khan, S., & Naghman, N. F. (2025). AI Assisted Heart Disease Prediction and Classification and Segmentation based on PIMA and UCI Machine Learning Datasets. Annual Methodological Archive Research Review, 3(7), 248-276.

Gul, W., Nawaz, A., Hamaz, M. T., & Khan, H. AN EFFICIENT MODEL FOR THE SELECTION OF LEADERSHIP COMPETENCIES AND PERFORMANCE IMPROVEMENT FOR THE SUCCESS OF TRANSPORTATION PROJECTS, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES Vol.-16, No.-5, May (2021) pp 49-65 https://doi.org/10.26782/jmcms.2021.05.00005

Gularte, K.H.M.; Vargas, J.A.R.; Da Costa, J.P.J.; Da Silva, A.A.S.; Santos, G.A.; Wang, Y.; Müller, C.A.; Lipps, C.; Júnior, R.T.S.; Vidal Filho, W.B.; et al. Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape through Systematic Literature Review. IEEE Access 2024, 12, 72871–72895.

Gupta, H., et al. (2021). 'Secure Cloud Storage for Healthcare using Blockchain.' Journal of Medical Systems.

H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

Hamayun Khan,Sheeraz Ahmed,S. Farhan Haider Shah,Rehan Ali Khan,Zeeshan Najam,Hasnain Abbas,Asif Nawaz,Zubair Aslam Khan, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES Vol.-15, No.-8, August (2020) pp 628-646 https://doi.org/10.26782/jmcms.2020.08.00053

Hasan, Md. K., et al. "Big Data and IoT: Security and Storage Challenges." arXiv, 2021.

Hashmi, U., & ZeeshanNajam, S. A. (2023). Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

Hassan, A., Khan, H., Ali, A., Sajid, A., Husain, M., Ali, M., ... & Fakhar, H. (2024). An Enhanced Lung Cancer Identification and Classification Based on Advanced Deep Learning and Convolutional Neural Network. Bulletin of Business and Economics (BBE), 13(2), 136-141.

Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

He, Y., Yu, F. R., Zhao, N., Yin, H., Yao, H., & Qiu, R. C. (2016). Big data analytics in mobile cellular networks. IEEE access, 4, 1985-1996.

HIPAA (1996). Health Insurance Portability and Accountability Act. U.S. HHS.

Hornyack, P., et al. (2011). 'AppFence: Toward usable privacy for Android.' USENIX Security Symposium.

Hossain, M., et al. "IoT-Enabled Teleconsultation in Healthcare." Springer Telemedicine, 2021.

Hu, J., & Vasilakos, A. V. (2016). Energy big data analytics and security: challenges and opportunities. IEEE Transactions on Smart Grid, 7(5), 2423-2436.

Hussain, M., Ahmed, H. A., Babar, M. Z., Ali, A., Shahzad, H. M., Rehman, S. U., ... & Alshahrani, A. M. (2025). An Enhanced Convolutional Neural Network (CNN) based P-EDR Mechanism for Diagnosis of Diabetic Retinopathy (DR) using Machine Learning. Engineering, Technology and Applied Science Research, 15(1), 19062-19067.

Hussain, S., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). An Enhanced Random Forest (ERF)-based Machine Learning Framework for Resampling, Prediction, and Classification of Mobile Applications using Textual Features. Engineering, Technology & Applied Science Research, 15(1), 19776-19781.

Imtiaz, M. A., Amir, A., Bakhet, S., Siddique, H., & Rizwan, S. M. (2025). An Optimal Diabetic Retinopathy Detection and Classification Approach based on integrated Hybrid Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(2).

Islam, S. M. Riazul, et al. "The Role of IoMT and Big Data in Modern Healthcare." Journal of Network and Computer Applications, Elsevier, 2022.

Ismaeel, S., Saleemi, H., Amir, U., Ashraf, S., & Hamza, A. (2024). A Detailed Review of latest Trends, Technologies Applications

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), 143-161.

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M.F. and Naqvi, S.A.A., 2025. Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), pp.143-161.

Javed, M. A., Ahmad, M., Ahmed, J., Rizwan, S. M., & Tariq, A. (2025). An Enhanced Machine Learning based Data Privacy and Security Mitigation Technique: An Intelligent Federated Learning (FL) Model for Intrusion Detection and Classification System for Cyber-Physical Systems in Internet of Things (IoTs). Spectrum of Engineering Sciences, 3(2), 377-401.

Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

Khan, A. K., Bakhet, S., Javed, A., Rizwan, S. M., & Khan, H. (2025). Framework for Predicting Customer Sentiment Aware Queries and Results in Search Using Oracle and Machine Learning. Spectrum of Engineering Sciences, 3(2), 588-617.

Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core

Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

Khawar, M. W., Ayub, N., Shaheen, S., Iftikhar, B., Masood, H., Ahmad, A., & Khan, H. (2025). An Efficient system based on Artificial Intelligence for the Detection and Mitigation of network Intrusion using encrypted traffic protocols: A Systematic Approach. Annual Methodological Archive Research Review, 3(11), 32-71.

Khawar, M. W., Salman, W., Shaheen, S., Shakil, A., Iftikhar, F., & Faisal, K. M. I. (2024). Investigating the most effective AI/ML-based strategies for predictive network maintenance to minimize downtime and enhance service reliability. Spectrum of Engineering Sciences, 2(4), 115-132.

Kumar, Neeraj, et al. "IoT Security Challenges in 5G Healthcare." Springer, 2020.

Li, H.; Luo, L.; Wang, H. Federated learning on non-independent and identically distributed data. In Proceedings of the Third International Conference on Machine Learning and Computer Application (ICMLCA 2022), Shenyang, China, 16–18 December 2023; SPIE: Bellingham, WA, USA; pp. 154–162.

Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

Liaqat, M. S., Sharif, N., Ali, A., Khan, H., Ahmed, H. N., & Khan, H. (2024). An Optimal Analysis of Cloud-based Secure Web Applications: A Systematic Exploration based on Emerging Threats, Pitfalls and Countermeasures. Spectrum of engineering sciences, 2(5), 427-457.

Liu, Y., et al. (2020). 'Shadow Coding for Privacy-Preserving Data Aggregation.' IEEE Transactions.

M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

Mahmood, F., Shehroz, M., Ansari, Z., & Rauf, F. (2024). A Survey of Software-Defined Networks Based on Advance Machine Learning Based Techniques. Spectrum of Engineering Sciences, 2(4), 232-257.

Maqsood, M., Dar, M. M., Javed, M. A., & Khan, H. (2024). A Survey on the Internet of Medical Things (IOMT) Privacy and Security: Challenges Solutions and Future from a New Perspective. The Asian Bulletin of Big Data Management, 4(4), 355-368.

Mittal, R., et al. (2018). 'Homomorphic Encryption in Cloud Health Environments.' ACM Computing Surveys.

Muhammad Anas,Muhammad Atif Imtiaz,Saad Khan,Arshad Ali,Noor Fatima Naghman,Hamayun Khan,Sami Albouq, AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING, Cont.& Math. Sci, Vol.20, No.3, 2025 https://doi.org/10.26782/jmcms.2025.03.00005

Mujtaba, A., Zulfiqar, M., Azhar, M. U., Ali, S., Ali, A., & Khan, H. (2025). ML-based Fileless Malware Threats Analysis for the Detection of Cyber security Attack based on Memory Forensics: A Survey. The Asian Bulletin of Big Data Management, 5(1), 1-14.

Mumtaz, J., Bakhet, S., Javed, A., Naz, A., Rashail, M., & Khan, H. (2025). An Intelligent Diagnosis and Tumor Segmentation Method based on MRI Images Using Pre-trained Deep Convolutional Neural Networks (CNNs). The Asian Bulletin of Big Data Management, 5(1), 147-163

Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

Musharraf, S. T., Masab, M. M., Ayub, N., Murtaza, S., Ullah, H., Ahmad, A., ... & Khan, H. (2025). An Efficient Artificial Intelligence-Based Early Prediction of Heart Attack Using Deep Learning CNN and SVM Models: https://doi. org/10.5281/zenodo. 17551611. Annual Methodological Archive Research Review, 3(10), 265-301.[121]. Kostkova, Patty, et al. "Ethics of Big Data in Healthcare: Balancing Innovation and Privacy." Philosophy & Technology, Springer, 2021.

Mustafa, M., Ali, M., Javed, M. A., Khan, H., Iqbal, M. W., & Ruk, S. A. (2024). Berries of Low-Cost Smart Irrigation Systems for Water Management an IoT Approach. Bulletin of Business and Economics (BBE), 13(3), 508-514.

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

Nawaz, S., Salman, W., Shahid, U., Khokhar, M. L., Iqbal, M. Z., & Hamid, A. (2024). A Survey on Latest Trends and Technologies of Computer Systems Network. Spectrum of Engineering Sciences, 2(4), 85-114.

Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

Niaz, H. U., Qadeer, Q. B. Q., Niaz, H., Mansib, H., Awais, M., & Khan, H. (2025). Artificial Intelligence Assisted Autonomous Unmanned Aerial Vehicles (UAVs) and Aerial drones based on Machine Vision for Enhancing Remote Sensing of Precision crop Health Monitoring. The Asian Bulletin of Big Data Management, 5(4), 155-177.

Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

Pham, Q.-V., et al. "AI and Big Data for COVID-19 Pandemic." arXiv, 2021.

Rafay, A., Salman, W., Yahya, G., & Malik, U. (2024). SD Network based on Machine Learning: An Overview of Applications and Solutions. Spectrum of Engineering Sciences, 2(4), 150-165.

Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

Raza, A., Khan, H., & Rehman, S. U. (2023). Computational Analysis of Nanomaterials for Energy Storage. International Journal of Advanced Sciences and Computing, 143-154.

Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

Shaikh, M. S. "Blockchain Applications for Secure Healthcare Big Data." Healthcare, MDPI, 2025.

Sodhro, A. H., et al. "Wearable IoT for Remote Patient Monitoring." IEEE Sensors Journal, 2020.

Sultan, H., Rahman, S. U., Munir, F., Ali, A., Younas, S., & Khan, H. (2025). Institutional dynamics, innovation, and environmental outcomes: a panel NARDL analysis of BRICS nations. Environment, Development and Sustainability, 1-43.

U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

Ullah, Sana, et al. "Wireless Body Area Networks: Applications and Challenges." Springer Healthcare IoT, 2020.

Waleed, R., Ali, A., Tariq, S., Mustafa, G., Sarwar, H., Saif, S., ... & Uddin, I. (2024). An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications. Bulletin of Business and Economics (BBE), 13(2), 200-206.

Xie, J., et al. (2020). 'Blockchain for Electronic Health Records: A Systematic Review.' IEEE Access.

Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic

Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

Yousaf, M., Khalid, F., Saleem, M. U., Din, M. U., Shahid, A. K., & Khan, H. (2025). A Deep Learning-Based Enhanced Sentiment Classification and Consistency Analysis of Queries and Results in Search Using Oracle Hybrid Feature Extraction. Spectrum of Engineering Sciences, 3(3), 99-121.

Zaheer, M., Azeem, M. H., Afzal, Z., & Karim, H. (2024). Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT. Spectrum of Engineering Sciences, 2(5), 458-479.

Zhang, R., et al. (2023). 'Federated Learning in Medical Imaging.' Nature Biomedical Engineering.

Zhang, Y., Zhang, L., Oki, E., Chawla, N. V., & Kos, A. (2017). IEEE access special section editorial: Big data analytics for smart and connected health. IEEE Access, 4, 9906-9909.

Zhou, J., et al. (2019). 'Privacy-Preserving Data Collection in Healthcare.' Health Informatics Journal.