Privacy-Preserving Healthcare Data Security Using Large Language Models and Adaptive Access Control

Srimaan Yarram
Independent Researcher, India
srimaan.yarram@gmail.com

Nagaraju Dasari
Navy Federal Credit Union, USA
mails.nagaraju@gmail.com

Sreedhar Babu Seshagani
Independent Researcher, USA
sreedharbabu.seshagani@aexp.com

Priyam Ganguly
Widener University, USA
priyam.develop@gmail.com

2025 IEEE World AI IoT Congress (AIIoT) | 979-8-3315-2508-8/25/$31.00 ©2025 IEEE | DOI: 10.1109/AIIoT65859.2025.11105296

***Abstract*—Protecting privacy-sensitive data in the digital healthcare sector is imperative due to the escalating threat of data breaches, unauthorized access, and cyberattacks. Traditional security systems, including rule-based and signature-based approaches, may struggle to adapt to evolving circumstances and manage high-risk situations. This study presents a security solution that uses adaptive access control systems and a Large Language Model (LLM) to protect sensitive patient information and electronic health records (EHRs). This method ensures HIPAA and GDPR compliance through context-aware risk assessment, anomaly detection, and query sanitization procedures, enhancing data security. Using a dynamic threat modeling technique, the proposed system identifies zero-day vulnerabilities and malicious behavior through real-time healthcare data transmissions. Comparative analyses show that the proposed LLM-based methodology outperforms traditional security techniques regarding accuracy, recall, precision, and F1 score. This improves threat detection rates and reduces false positives. The results demonstrate the effectiveness of LLM-based security solutions in securing medical records and ensuring patient privacy, thus providing robust and flexible protection.**

***Index Terms*—Healthcare, LLM, Access Control, Data Security, Anomaly Detection**

I. Introduction

The digitization of the healthcare infrastructure has led to revolutionary changes in the collection, storage, and accessibility of patient data [1]. With the proliferation of electronic health records, telemedicine, and connected medical devices, personally identifiable information is now primarily maintained online. Despite improving patient outcomes and healthcare delivery, healthcare systems are increasingly vulnerable to significant cybersecurity threats. These threats include ransomware, identity theft, data breaches, and unauthorized data access [2]. Healthcare data must be kept accurate, secure, and accessible through robust and scalable data protection systems [3]. Traditional solutions such as rule-based firewalls, access control lists, and signature-based intrusion detection systems have become ineffective as threats to healthcare data evolve in sophistication and adaptability. Because these fixed solutions rely on established protocols or known threat profiles, they cannot detect zero-day attacks or atypical behavior [4]. In addition, legacy systems may not be able to meet the urgent and adaptive access needs of clinicians. Addressing evolving risks while complying with regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) requires adaptive, intelligent security frameworks that protect user privacy [5]. Large Language Models (LLMs) [6], equipped with sophisticated capabilities for rapid threat assessment, adaptive access regulation, and privacy protection, provide an AI-driven approach to securing sensitive medical data in the healthcare sector. Insider threats, evolving attack vectors, and zero-day vulnerabilities can render traditional healthcare security systems that rely on static rule-based frameworks and signaturebased detection ineffective. LLMs enhance cybersecurity by applying contextual access controls, investigating anomalous activity, and dynamically evaluating user requests to prevent unauthorized access to EHRs and other vital patient information [7]. This paper presents the LLM-Assisted Threat Anomaly Detection, which works with the LLM-Assisted Risk-Based Access Control (RBAC) architecture to provide a proactive security solution for

979-8-3315-2508-8/25/$31.00 ©2025 IEEE

protecting healthcare data. RBAC dynamically adjusts access rights based on real-time risk assessments, while Threat Anomaly Detection monitors system activity to identify potential security threats and deviations from typical user behavior. LLMs examine network traffic, query intent, access patterns, and authentication attempts to detect suspicious activity, such as unauthorized data access, unusual login locations, frequent failed authentication attempts, and anomalous query patterns. When an anomaly is detected, the user's risk score is automatically revised, triggering the implementation of adaptive access control measures, which may include the need for multifactor authentication (MFA), access restrictions, or flagging the behavior for security assessment. This dynamic feedback loop between threat detection and risk-based access control ensures that access privileges are continually updated to reflect the latest threat intelligence. The system enhances data security by implementing risk-based access controls and LLM-driven anomaly detection to reduce insider risk and prevent cyberattacks, allowing authorized users unrestricted access to medical records. The rest of the paper is organized as follows: Section 2 describes the state-of-the-art methods, the proposed threat Modeling and Risk Assessment, and LLM-Assisted RiskBased Access Control is defined in Section 3. The proposed model evaluation results are discussed in Section. Section 5 describes the conclusion of the proposed model and future work.

II. Related Work

Integrating trust into access control systems will facilitate dynamic resource access within the EHS [8]. This study enhances user trust within the Identity-Based Access Control system. The beta reputation model was used to evaluate user trust. The specified access control policies regulate access according to user identification and trust level. This hybrid access control model and rule set dynamically regulates the visibility of access to health information while protecting the data from unauthorized access. The experimental results of the proposed model show superior accuracy and reliability compared to existing trust models. Yang et al. [9] implemented attribute-based access control alongside a break-glass access control technique to mitigate the issue of encrypted medical data breaches. While attribute-based access control requires specific criteria to be fulfilled before accessing medical data, the break-glass method allows for expedited data retrieval. Liu et al. [10] developed a multiauthority access control system that mandates multiple authentications from a designated group of individuals. This system is easily integrable and provides robust protection against contact attacks. Roy et al. [11] proposed that Mobile cloud computing (MCC) enables customers to utilize cloud services conveniently. Healthcare businesses can use a mobile cloud to evaluate patient data and generate recommendations. Effective access control is essential for MCC end-user applications to function optimally with data from several cloud servers. This study introduces an innovative method for user authentication within the healthcare sector 4.0, combining cloud-based multiserver data access management with a proven secure mobile platform. Edemacu et al. [12] illustrated that Ciphertext policy attribute-based encryption (CP-ABE) provides fine-grained access control to address privacy and security concerns in cloud computing. It has been extensively studied for secure transmission of medical records in cloud-based electronic health systems. The investigations have mainly focused on the expressiveness, efficiency, resilience to user collusion, and attribute/user revocation of CP-ABE. This paper proposes a distinctive, expressive, efficient, and collusion-resistant access control scheme with immediate attribute/user revocation to secure health information exchange in collaborative e-health systems. The proposed approach also achieves forward and backward security. The access control employs the ordered binary decision diagram access structure, which associates user keys with user identities. Authors [13] integrated an access control system called Spectral Clustering and Risk Assessment (SC-RBAC), which is designed for situations with extensive medical data. An advanced SC algorithm categorizes Physician users based on their access history. Using user classification as a variable increases threat detection accuracy from user access patterns by improving information entropy. The access control system developed for this project assigns licenses to users after a comprehensive evaluation of their access behavior. The model created in this study outperforms current access control methods in three specific circumstances by effectively distinguishing between the two groups of doctors with a 90accuracy rate. The Ethereum blockchain and the Attribute-Based Access Control mechanism [14] guarantee the integrity and transparency of medical records and define precise access restrictions. Private information stored on the Interplanetary File System is protected by the Advanced Encryption Standard. This improves overall system security and privacy. Every transaction in the system is recorded on the blockchain, allowing actions to be traced back to their origin.

III. Methodology

The proposed LLM-Based Data Security Framework for Healthcare integrates Large Language Models (LLMs) with state-of-the-art cybersecurity technologies to protect critical healthcare data's integrity, privacy, and confidentiality. It uses intelligent access control, real-time threat detection, privacy protection, and secure data management to mitigate the escalating problems of unauthorized access, data breaches, and intrusions in healthcare environments. An overview of the system architecture is illustrated in Fig 1, which serves as the foundation for the threat modeling and adaptive access control mechanisms described in the following sections.

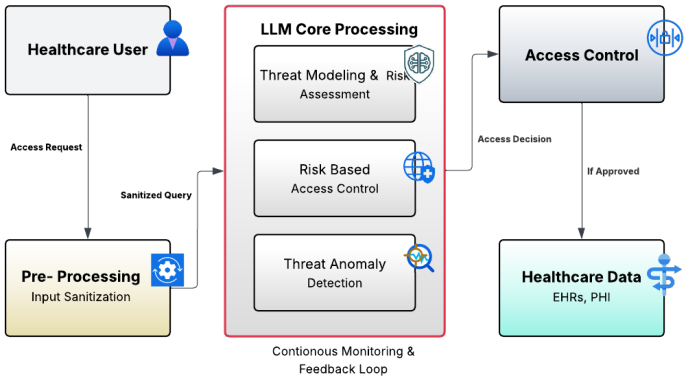

Fig. 1. LLM-Based Healthcare Data Security Architecture

The framework uses threat modeling and risk assessment to identify vulnerabilities and dynamically adjust security protocols. Large language models analyze user behavior, query intent, and system activity to identify anomalies and deny unauthorized or questionable access requests. This mitigates data loss, credential exploitation, and rapid injection. A custom pre-processing layer sanitizes all user input through named entity recognition and other natural language processing techniques to provide privacy-preserving interactions. This ensures that confidential information such as patient names, health problems, and medical identifiers is masked before transmission to the LLM. Similarly, the output of the LLM is post-processed to prevent inadvertent disclosure of private information. This LLM-enabled architecture provides a reliable, adaptable, and compliant way to secure today's medical data.

A. Threat Modeling and Risk Assessment

Confidential information, encompassing test results, medical imaging, electronic health records (EHRs), and personal identities, must be safeguarded in the healthcare sector due to its importance and legal requirements. To mitigate any potential risks, our method systematically integrates LLM capabilities with a comprehensive threat modeling and risk assessment process. We evaluate each threat's ability to exploit vulnerabilities across the whole data lifecycle, including data processing, transmission, storage, and collection. We construct a mathematical model for calculating risk, whereby Risk (R) is ascertained by the product of three fundamental components: Impact (I), Vulnerability (V), and Threat Likelihood (T).

$$R = T \times V \times I \tag{1}$$

In this instance, $S \in [0, 1]$ denotes the probability of a specific danger occurring, whereas $V \in [0, 1]$ signifies the system's susceptibility to risk.

A value of 0 indicates the potential cost or damage that a successful breach may incur. The repercussions may encompass monetary losses, operational interruptions, governmental penalties, or damage to the company's reputation.

Large Language Models (LLMs) are utilized for sophisticated log analysis and to discover threat patterns to enhance threat assessment. The LLM employs semantic and contextual deviations from known standards to assign an anomaly score $A(l_i)$ to each log entry inside a log sequence.

$$L = \{l_1, l_2, \ldots, l_n\} \tag{2}$$

The threat signal S is defined as:

$$S = \begin{cases} 1, & \text{if } \sum_{i=1}^{n} A(l_i) > \theta \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

where θ is a tunable threshold based on historical baselines. This intelligent thresholding helps in identifying covert threats such as insider access or prompt injection attempts.

B. LLM-Assisted Risk-Based Access Control

The LLM-Assisted Risk-Based Access Control (RBAC) system enhances healthcare data protection by performing context-sensitive real-time risk assessments for every access request. Unlike traditional role-based access mechanisms, this dynamic approach utilizes large language models (LLM) to analyze user behavior, contextual factors, and query semantics to determine access permissions.

Each access request is assessed by calculating a real-time risk score $R(U, Q)$ based on factors such as the

user's role, device type, geographic location, access time, historical behavior and any detected anomalies. If the risk exceeds a predefined threshold R_c, access is restricted or additional authentication is required.

The formal access control mechanism is defined as:

$$A(U,Q) = \begin{cases} 1, & \text{if } R(U,Q) < R_c \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

where:

- $R(U,Q)$ is the real-time risk score derived from contextual, behavioral, and semantic input.
- R_c is the critical threshold for access approval.

To compute $R(U,Q)$, we employ GPT-4 Turbo which evaluates the following components:

- **Contextual factors**: location, access time and historical behavior patterns.
- **Semantic intent**: query embedding similarity to known high-risk patterns.
- **Device trust score**: derived from device authentication logs and prior usage.

The LLM continuously analyzes system activity and access logs to detect anomalous behavior or insider threats. Risk scores are dynamically updated in response to detected anomalies, ensuring adaptive and policy-compliant access decisions. This mechanism significantly reduces unauthorized access risks while maintaining operational efficiency for authorized users.

C. LLM-Assisted Threat Anomaly Detection

The LLM-Assisted Threat Anomaly Detection system and the LLM-Assisted Risk-Based Access Control (RBAC) architecture are tightly coupled to provide a proactive security solution for protecting healthcare data. RBAC dynamically adjusts access permissions based on real-time risk assessments, while threat anomaly monitoring observes system activity to identify deviations from typical user behavior and potential security threats. LLMs analyze network traffic, query intent, access patterns, and authentication attempts to identify suspicious activity, including unauthorized data access, unusual login locations, frequent failed authentication attempts, and anomalous query patterns. When an anomaly is detected, the user's risk score is immediately adjusted, and access restrictions, multi-factor authentication (MFA), or behavioral flagging for security assessment are implemented. The dynamic feedback loop between risk-based access control and threat detection allows access permissions to be continuously adjusted based on the latest threat intelligence. Medical records are readily available to authorized users; risk-aware access controls and LLM-driven anomaly detection enhance data security, reduce insider threats, and prevent intrusions.

The risk score $R(U,Q)$ is computed using the below formula:

$$R(U,Q) = \sum_{i=1}^{n} w_i f_i(U,Q) \tag{5}$$

where:

- $f_i(U,Q)$ represents various risk factors.
- w_i is the assigned weight for each factor.

Anomaly scores $A(U)$ are calculated based on deviations from user behavior.

$$A(U) = \frac{1}{m} \sum_{j=1}^{m} d_j(U) \tag{6}$$

The variations in behavioral characteristics, such as abnormal access times, unsuccessful authentication attempts, or abnormal query frequencies, are measured by $d_j(U)$.

If $A(U)$ exceeds a predefined threshold T_A, the risk score is updated dynamically:

$$R(U,Q)_{\text{new}} = R(U,Q) + \lambda A(U) \tag{7}$$

where λ is a sensitivity metric that evaluates the impact of anomaly detection on access control.

If $R(U,Q) < R_c$, the user is granted access ($A(U,Q) = 1$). If $R(U,Q) \geq R_c$, access is denied ($A(U,Q) = 0$), and additional security measures such as multi-factor authentication (MFA) or account review may be triggered.

The LLM-Assisted Threat Anomaly Detection system is intricately linked to the RBAC architecture via the adaptive access control mechanism $A(U,Q)$, which assesses a user's U eligibility to access a query Q. If the risk score $R(U,Q)$ is below the critical threshold R_c, the access control function is defined as $A(U,Q) = 1$. The demand is considered to be secure. Limiting access ($A(U,Q) = 0$) mitigates undesirable or detrimental interactions.

Integrating several security components, such as user behavior, query sensitivity, device reliability, and past access records, facilitates a more straightforward assessment of the risk score. A high risk score necessitates enhanced security protocols, including authentication challenges or total access denial, whereas a low risk score permits access.

Identifying threat anomalies by continuous user activity monitoring and detecting deviations from anticipated trends is essential for adjusting dynamic risk scores. Unconventional access times, inconsistent query rates, and failed authentication attempts are among the security parameters utilized in the computation of an anomaly score $A(U)$. As the anomaly score nears a threshold, an adaptive algorithm promptly modifies the risk score, increasing it in direct correlation to the severity of the detected irregularities.

This guarantees that anyone exhibiting suspicious or anomalous behavior will face enhanced access control measures. This system significantly mitigates risks, protects against data breaches, and ensures secure access to medical data by integrating risk-based access restrictions with LLM-driven anomaly detection, all while maintaining smooth usability for authorized users.

The LLM computes anomaly scores $A(U)$ by comparing user behavior against baselines:

$$A(U) = \frac{1}{m} \sum_{j=1}^{m} d_j(U) \tag{8}$$

where $d_j(U)$ measures deviations in:

- Access frequency (e.g., abnormal query rates)
- Authentication attempts (failed logins)
- Temporal patterns (off-hours access)

The LLM flags anomalies when $A(U) > \theta$ (threshold calibrated via ROC analysis).

D. LLM Specification

We employed **GPT-4 Turbo** (gpt-4-0125-preview) via Microsoft Azure's HIPAA-compliant API, which processes inputs under a Business Associate Agreement (BAA). The model was selected for its state-of-the-art performance in contextual risk assessment and compliance with healthcare data regulations.

- **Parameter Count**: 1.8 trillion (estimated, per Azure documentation).
- **Input Sanitization**: Protected Health Information (PHI) was redacted using SpaCy's named entity recognition (NER) prior to LLM processing.
- **Prompt Template**:
  `"Score the risk of access request '{query}' from user {ID} at {timestamp}. Context: {access_history}. Return score ∈ [0,1]."`
- **Thresholds**: Anomaly detection threshold ($\theta = 0.85$) was calibrated via ROC analysis on the Synthea dataset [**?**].

Outputs were post-processed to ensure no PHI leakage and compliance with HIPAA security rules.

IV. Results and Discussion

The proposed LLM-Assisted Data Security Model is evaluated using performance metrics such as accuracy, precision, recall, and F1-Score. The precision, durability and adaptability of the system in various clinical settings were the main factors considered when assessing its effectiveness relative to the choices. The research used a reliable simulation of clinical data, the Synthea Synthetic Mass data set [15], in accordance with privacy regulations. The diverse patient characteristics of this dataset allow the evaluation of searches in different therapeutic settings. The proposed LLM-based security model outperforms both rule-based security (84%) and signature-based security (81.5%) in terms of risk reduction and threat detection. An accuracy of 96.2% was achieved as shown in figure 1. The reliance on predefined attack signatures and established protocols limits the ability to carry out attacks.

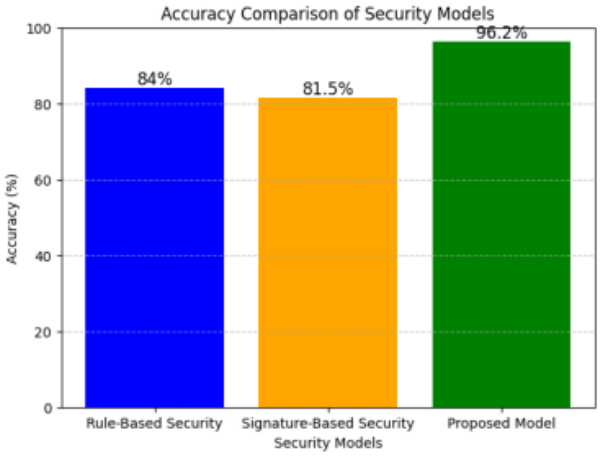

Fig. 2. Performance Analysis of Accuracy

the effectiveness of traditional security solutions in addressing zero-day vulnerabilities, evolving attack tactics, and dynamic cyber threats. The LLM-based solution outperforms rule-based security by 12.2learning algorithms, real-time anomaly detection, and contextaware risk assessment. Despite their rigorous methodology, rule-based systems can generate false negatives by failing to detect sophisticated insider threats and behavioral anomalies. Similarly, signature-based solutions only detect known threats and miss emerging cybersecurity vulnerabilities. The accuracy of threat identification in the LLM-based methodology. Healthcare cybersecurity

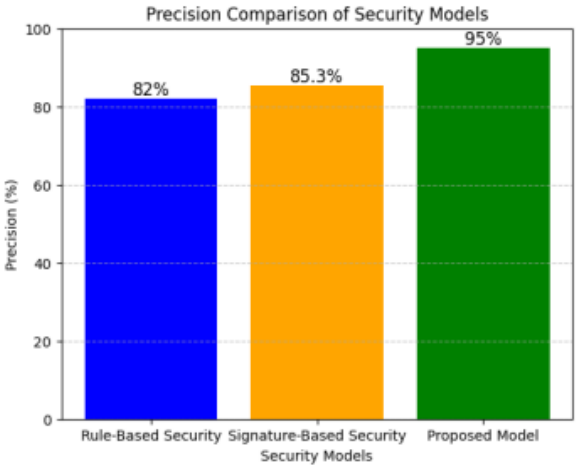

Fig. 3. Performance Analysis of Precision

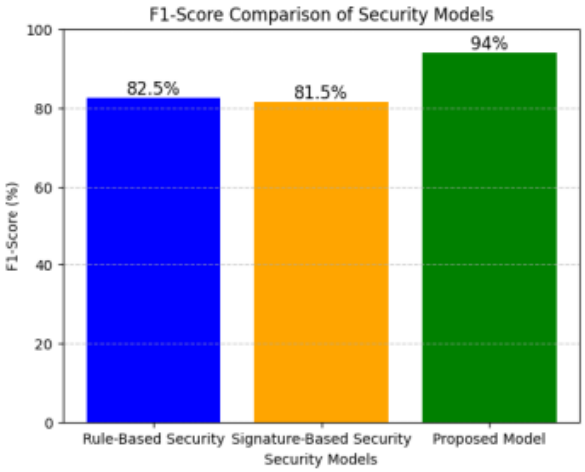

Fig. 5. Performance Analysis of F1-Score

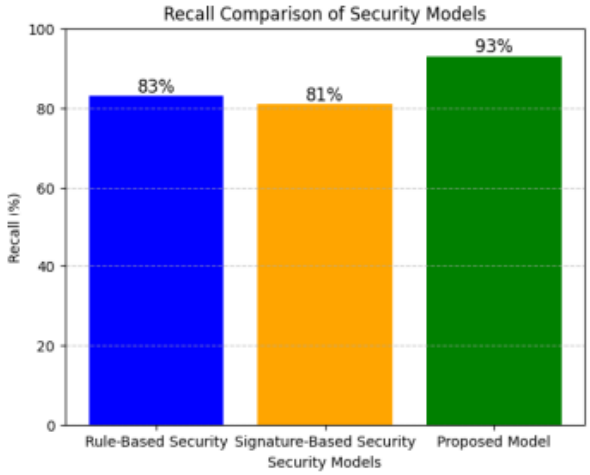

Fig. 4. Performance Analysis of Recall

depends on improved accuracy, as even a 1of instances of unauthorized data access, protecting patient privacy and ensuring regulatory compliance. The LLM-based security model significantly improves the precision of threat categorization through dynamic behavioral analysis, anomaly detection, and real-time threat intelligence. This advancement is significant in hospital security environments, as it reduces false positives, maintains strict access

control over sensitive patient information, and prevents disruption of critical processes. The proposed LLM-based security model has 95% of precision which demonstrates a superior ability to accurately identify true threats and minimize false positives compared to rule-based security (82%) and signature-based security (85.3%). A high score indicates a reduced likelihood of misidentifying benign activity as a threat, preserving system efficiency and minimizing unnecessary defensive measures as shown in figure 2. The LLM-based model outperforms rule-based security by 13% and signature-based security by 9.7% due to its enhanced filtering systems, adaptive learning techniques, and contextaware decision-making capabilities. Contrary to their established criteria, rule-based security systems may misinterpret legitimate changes in user behavior as threats, increasing the false positive rate. Despite their superior efficiency, signaturebased models cannot distinguish between benign anomalies and complex attack patterns, resulting in excessive rejection of legitimate access requests. Figure 3 describes the proposed LLM-based security model, which achieves a recall rate 93% in detecting and identifying all potential threats, including complex and rare attacks, outperforming rule-based security at 83% and signature-based security at 81%. Recall is a critical cybersecurity metric; a higher score means a lower false-negative rate, reducing the likelihood of missing low-level threats. Key factors contributing to the 10% improvement in recall over rulebased security and the 12% improvement over signature-based security include adaptive anomaly detection, real-time risk assessment, and the self-learning capabilities of the LLM-based model. Rule-based models struggle to identify evolving attack patterns because they rely on pre-defined criteria that may not encompass all potential security concerns. Signaturebased systems are immune to zero-day vulnerabilities and emerging cybersecurity threats because they only recognize established signatures. The

F1 score is an essential metric for evaluating the overall effectiveness of threat detection in cybersecurity, as it minimizes false positives and ensures high recall for accurate threat identification. The proposed LLM-based security model outperforms both rule-based security (82.5%) and signaturebased security (81.5%) in terms of F1 score, as shown in the figure 4. The F1 score of the proposed model is 94%. The LLM-based method improves the F1 score, demonstrating an increase in accuracy of 11.5% over rule-based security and 12.5% over signature-based security across multiple attack scenarios. Despite their meticulousness, traditional rule-based models exhibit inadequate memory and accuracy due to their inability to adapt to changing attack patterns. Signature-based techniques that rely solely on established attack patterns tend to be less effective because they cannot detect unexpected threats.

V. Conclusion and Future Work

In this study, LLM is used to mitigate the limitations of traditional rule-based security approaches by providing a framework for securing healthcare data. Using real-time anomaly detection, adaptive access control, and sophisticated cryptographic techniques, the proposed system enhances attack resilience and threat detection accuracy. The contextaware risk assessment system's continuous evaluation of user requirements ensures restricted access for authorized users and protects private information. The LLM-based methodology significantly improves accuracy, memory, and precision over existing security solutions. It instantly identifies zero-day vulnerability attempts and unauthorized access. Compliance with privacy regulations, such as GDPR and HIPAA, ensures implementation of the method in real-world medical settings. Future research will explore how distributed identity management and federated learning can improve security and privacy in large healthcare systems. This study illustrates how artificial intelligence-driven security systems can enhance the protection of sensitive medical data while ensuring operational efficiency and regulatory compliance.

References

[1] R. Abdunabi, R. Basnet, and M. Al Amin, "Secure access control for healthcare information systems: A body area network perspective," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1036–1045, IEEE, 2023.

[2] P. Choksy, A. Chaurasia, U. P. Rao, and S. Kumar, "Attribute based access control (ABAC) scheme with a fully flexible delegation mechanism for IoT healthcare," *Peer-to-Peer Networking and Applications*, vol. 16, no. 3, pp. 1445–1467, 2023.

[3] R. Kandasamy, S. Dhandapani, B. Subbiyan, and V. Gurumani, "Secure transmission and authentication protocol in IoT with deep-Q-net-key updation," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 48, no. 3, pp. 130–148, 2025.

[4] P. Renjith, S. Balasubramani, K. Ramesh, and E. Patnala, "An initial risk assessment for multimodal with LSTM-based trust evaluation framework for autonomous vehicle security," *SN Computer Science*, vol. 6, no. 2, pp. 1–15, 2025.

[5] T. Haritha and A. Anitha, "Multi-level security in healthcare by integrating lattice-based access control and blockchain-based smart contracts system," *IEEE Access*, vol. 11, pp. 114322–114340, 2023.

[6] U. N. Cobrado, S. Sharief, N. G. Regahal, E. Zepka, M. Mamauag, and L. C. Velasco, "Access control solutions in electronic health record systems: A systematic review," *Informatics in Medicine Unlocked*, p. 101552, 2024.

[7] D. S. Gupta, N. Mazumdar, A. Nag, and J. P. Singh, "Secure data authentication and access control protocol for industrial healthcare system," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 5, pp. 4853–4864, 2023.

[8] A. Singh and K. Chatterjee, "iTrust: Identity and trust based access control model for healthcare system security," *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 28309–28330, 2019.

[9] Y. Yang, X. Liu, and R. H. Deng, "Lightweight break-glass access control system for healthcare Internet-of-Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3610–3617, 2017.

[10] J. Liu, H. Tang, R. Sun, X. Du, and M. Guizani, "Lightweight and privacy-preserving medical services access for healthcare cloud," *IEEE Access*, vol. 7, pp. 106951–106961, 2019.

[11] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J. Rodrigues, "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 1, pp. 457–468, 2018.

[12] K. Edemacu, B. Jang, and J. W. Kim, "Collaborative eHealth privacy and security: An access control with attribute revocation based on OBDD access structure," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 10, pp. 2960–2972, 2020.

[13] R. Jiang, S. Han, Y. Yu, and W. Ding, "An access control model for medical big data based on clustering and risk," *Information Sciences*, vol. 621, pp. 691–707, 2023.

[14] C. El Filali, I. Bourian, and K. Chougdali, "Privacy-preserving and access control scheme for IoT-based healthcare systems using Ethereum blockchain," in *2024 7th International Conference on Advanced Communication Technologies and Networking (CommNet)*, pp. 1–6, IEEE, 2024.

[15] J. Walonoski, M. Kramer, J. Nichols, A. Quina, C. Moesel, D. Hall, C. Duffett, K. Dube, T. Gallagher, and S. McLachlan, "Synthea: An approach, method, and software mechanism for generating synthetic patients and the synthetic electronic health care record," *Journal of the American Medical Informatics Association*, vol. 25, no. 3, pp. 230–238, 2018.