Cloud-Based Multi-Layer Security Framework for Protecting E-Health Records

P Ramesh Naidu[1]
Department of Computer Science and Engineering,
Nitte Meenakshi Institute of Technology, Bangalore, Karnataka, India.
ramesh.naidu@nmit.ac.in

Dankan Gowda V[2]
Department of Electronics & Communication Engineering,
BMS Institute of Technology and Management,
Bangalore, Karnataka, India.
dankan.v@bmsit.in

Ujwala Suryakant Mali[3]
Assistant professor, Applied Science,
Bharati vidyapeeth college of Engineering. Navi Mumbai, India.
ujwalla.mali@bvcoenm.edu.in

Shruti Mallikarjun[4]
Research Scholar, Department of Computer Science, Karnataka State Akkamahadevi Women University, Vijaypura, Karnataka, India.
shrutimp32@gmail.com

Srinivas.D[5]
Assistant professor, School of Business, SR University, Warangal, Telangana, India.
srinivas.d@sru.edu.in

Sheetalrani R Kawale[6]
Assistant Professor, Department of Computer Science, Karnataka State Akkamahadevi Women University, Vijayapura, Karnataka, India.
sheetalrkawale@gmail.com

2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI) | 979-8-3503-3091-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICAIIHI57871.2023.10489781

Abstract: - **The increasing role that cloud computing plays in storing e-health data has highlighted the necessity for strong security measures. The purpose of this study is to shed light on the difficulties in protecting private health data that is kept on cloud servers. As the first priority, we developed a unique multi-layer security architecture that is cloud-based to protect electronic health data. We provide a complete analysis of the current security protocols, perform a vulnerability assessment, and create a more robust multi-layered security architecture as part of our methodology. The concept includes sophisticated encryption methods, strict access rules, and instruments for ongoing threat detection. In order to assess the effectiveness of the framework, we ran extensive simulations with an emphasis on data integrity, access control, and confidentiality. The findings show a considerable improvement over conventional, one-layer security techniques. The proposed framework guarantees regulatory compliance in addition to providing enhanced security against illegal access and data breaches. We have found that safeguarding electronic health records—which are critical for both patients and healthcare providers—requires a multi-layered security approach built on the cloud. The findings of this study may lead to improved cloud-based healthcare data security in the future.**

Keywords: E-Health Records Protection, Multi-Layer Security Framework, Health Data Privacy, Data Integrity, Access Control Mechanisms.

I. INTRODUCTION

Electronic health records are progressively moving to cloud-based storage options in the ever-changing healthcare IT market. This modification presents significant security concerns in spite of its numerous benefits in terms of accessibility, scalability, and cost-effectiveness [1]. Electronic health records are susceptible to cyberattacks, there are issues with data integrity and confidentiality, and adhering to stringent healthcare regulations are just a few of the challenges in maintaining the security of these information in the cloud [2]. Because health data is vast and varied, and cloud computing is multi-tenant, the risks of data breaches and unauthorized access are increased. Given these concerns, it is essential to use a robust, multi-layered security approach to safeguard cloud-based electronic health data. Electronic health record security is more than a technology concern; it's a fundamental patient right that relies on confidence in healthcare systems [3]. Robust security measures are necessary for several reasons. To start, since e-health records include sensitive personal data, there is a chance of privacy violations and misuse. Second, as accurate diagnosis and treatment rely on the protection of health data, patient safety is directly impacted by it [4]. Observing regulations such as the Health Insurance Portability and Accountability Act is legally required, since healthcare providers are required to protect patient information [5]. Maintaining the security of electronic health information in the cloud is crucial to upholding the moral, legal, and professional standards of healthcare in a time when cyber threats are becoming more complex.

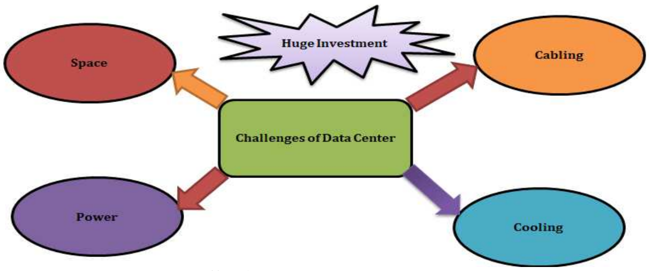

Figure.1: *Difficulties in Managing Data Centers*

A storage system serves as a framework that accommodates computer systems alongside other interconnected components, including communication and storage elements. It typically encompasses redundant or backup power sources, multiple data communication links, environmental control systems, and security mechanisms[6]. Figure 1 illustrates the challenges faced by physical data centers. The primary objective of a data center is to execute programs responsible for managing an organization's crucial business and operational data[7]. These systems can either be proprietary and developed in-house or acquired from corporate software vendors, with common applications including ERP and CRM systems. The initial intent of many current data centers was to service internal or devoted customers, which often causes problems with efficiency, scalability, and adaptability[8]. Due to the limitations imposed by their technical and architectural design, many data centers are unable to fulfill the increasing demands of external markets and internal expectations, mostly because they are reluctant to adopt new technologies such as cloud computing[9]. Concerns about the safety of electronic health records stored in the cloud have recently emerged as a major area of study. It's necessary to create a strong cloud-based multi-layer security system specifically to safeguard sensitive medical data. Ensuring adherence to healthcare regulations including GDPR and HIPAA, the framework aimed to enhance data availability, integrity, and security. The study was organized around many important goals in order to arrive at that conclusion. The investigation's primary goal was to identify existing security flaws and future development prospects in cloud-based electronic health record systems. The development of a more resilient security architecture was greatly aided by the study findings. Second, a multi-layer security paradigm was the study's intended goal. The objective of this strategy was to provide a more complete security solution than the single-layered systems that were already in use by including advanced encryption techniques, strong access controls, and ongoing threat monitoring protocols. A thorough testing and assessment of the final architecture's ability to mitigate various security vulnerabilities is required. The framework's compliance with data protection and regulatory compliance criteria, as well as its functionality in real-world application situations, were ascertained by the results of these tests. The study also sought to provide a precise and useful implementation plan for the framework. The goal of the approach was to define precise, measurable requirements that would make it easier for healthcare providers to effectively and practically integrate the framework into their current cloud-based systems. Our study's main objective was to fill a vacuum in the existing literature and provide a foundation for future developments in healthcare data security. The researchers anticipated that their findings will lead to more dependable and safer digital healthcare systems for both physicians and patients by addressing the shortcomings that now exist in cloud-based EHRs. By accomplishing these objectives and providing a robust solution to protect sensitive health information in this digital age, the research hopes to significantly contribute to healthcare data security.

II. LITERATURE REVIEW

Securing cloud-based electronic health records presents a variety of challenges and approaches. Nowadays, data is often protected while it is being stored or transported using encryption techniques, particularly Public Key Infrastructure (PKI) and Advanced Encryption Standards (AES)[10]. Two of the most crucial elements for limiting who may access what data are Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). Cloud services include standard-specific security features to ensure compliance with healthcare standards such as GDPR and HIPAA, which is widely acknowledged as vital.

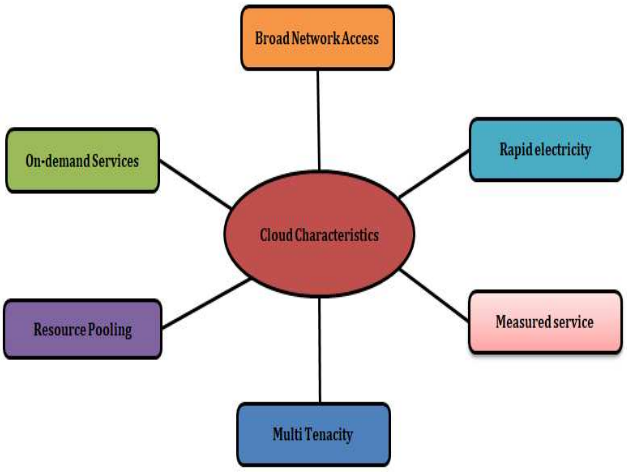

Figure.2: *Aspects of Cloud Computing*

Despite these improvements, there are still significant gaps in the literature. One major issue is scalability, which is essential for the ever-increasing amounts of healthcare data, but is a problem with many current security solutions [11]. There is a lot of untapped potential for predictive threat identification and real-time security improvements in the current state of security procedures that use AI and ML [12]. The lack of end-to-end security standards that address every facet of data processing is a common cause of security holes. The lack of regional security protocol standards further complicates the global interoperability of health data systems [13]. The human aspect is not given enough attention, which jeopardizes data integrity, particularly in terms of user awareness and security standard training. An first step towards resolving these problems might include developing a theoretical framework. The Information Security Management Theory (ISMT) emphasizes the significance of organizational controls and policies in the management of information security. One organized method for identifying and reducing risks in IT systems is the Risk Management Framework developed by the National Institute of Standards and Technology (NIST) [14]. The usefulness of common sense safety measures is illuminated by the Technology Acceptance Model (TAM), which helps us comprehend how people will react to cloud-based health systems [15]. The General Data Protection Regulation (GDPR)[16] establishes a thorough framework for privacy and data protection and provides guidelines for managing sensitive health data. The Cloud Security Alliance's (CSA) standards may provide best practices and suggestions for cloud computing security connected to healthcare data. The introduction of cloud computing, which provides networking, database, storage, and application solutions over the internet, has completely changed how users may access essential services. This innovative method significantly enhances performance and resource storage. Figure 2 [17] illustrates visually the scalability, accessibility, and efficiency that characterize cloud computing. This technology empowers users by streamlining access to a variety of services, which is advantageous to both consumers and companies [18,19]. The benefits and drawbacks of cloud-based e-health record security are covered in this research study. It emphasizes the need for a multi-layered security architecture that is scalable, user-focused, and able to change with the rapidly changing landscape of the digital healthcare industry. Additionally, this architecture has to be able to meet the needs of modern security threats.

III. METHODOLOGY

To build and assess the Cloud-Based Multi-Layer Security Framework for E-Health Record Protection, a comprehensive and multifaceted approach is planned. The study first thoroughly examines the literature to determine existing security practices and pinpoint vulnerabilities in cloud-based electronic health record systems before developing the security architecture. The intricacies of the multi-layer security architecture are worked out in the ensuing design phase. The main goals of this phase's work are to ensure that the strong access controls, ongoing threat monitoring, advanced encryption techniques, and compliance with healthcare data security regulations are all satisfied. A cloud simulation prototype may be built to assess the framework's performance [20]. This prototype is used to assess the system's functionality, resistance to cyberattacks, and compliance with laws such as GDPR and HIPAA. In addition, UAT involves healthcare professionals who evaluate the framework's usefulness and functionality in real-world situations. E-medicine stands at the forefront of contemporary e-health research. Electronic Medical Records (EMRs), encompassing medical data, images, and multimedia content, are seamlessly transmitted across potentially insecure connections to remote clinicians within the E-medicine service[21]. The healthcare cloud architecture greatly streamlines the gathering and management of patient information, particularly as patients move between different healthcare facilities, ensuring that their data remains accessible and traceable[22]. This healthcare cloud infrastructure leverages cloud technology to facilitate communication among healthcare service providers[23]. The internet has brought numerous advantages to the healthcare industry, encompassing both hardware and software enhancements. Figure 3 illustrates the integration of IoT devices and the communication networks within the e-health cloud, marking a significant advancement in healthcare technology.

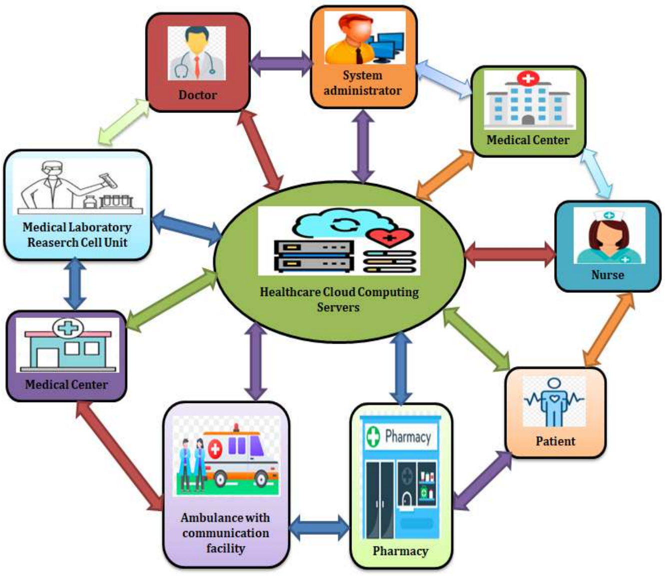
Doctor
System administrator
Medical Center
Medical Laboratory Reaserch Cell Unit
Healthcare Cloud Computing Servers
Nurse
Medical Center
Patient
Ambulance with communication facility
Pharmacy
Pharmacy

Figure.3: *Healthcare Leveraging Cloud Technology*

Deduplication is a method employed to eliminate redundant data within a dataset. An evaluation tool for deduplication identifies surplus copies of data and safely removes them through a deduplication process, resulting in the preservation of a single version[24]. Deduplication software scans data for duplicate byte sequences, ensuring the accuracy and suitability of a single-byte pattern before designating it as a reference[25].

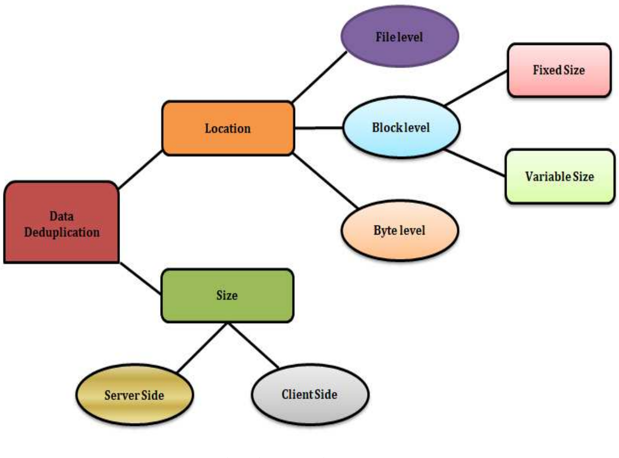

Figure.4: *Redundancy Elimination Categories*

Any subsequent attempts to save the same byte sequence will point back to the previously stored byte pattern. At a more advanced level, deduplication identifies and eliminates redundant data segments that may be the same, even if the containing files are not identical. Block-level deduplication, also referred to as sub-file deduplication, optimizes storage capacity[26]. While most block-level deduplication occurs at predefined block boundaries, variable-length deduplication or variable block deduplication can also break down data at non-fixed block boundaries. The various types of deduplication methods are depicted in Figure 4. Data collection is multifaceted, encompassing a thorough review of academic and industry literature, expert interviews to gather insights from professionals specializing in healthcare data and cloud security, and case studies of existing cloud-based e-health systems[27]. Data collected from the prototype testing, such as security event logs, system performance metrics, and user input, supplements this.

The acquired data is analyzed in an equally varied manner. The framework's performance is evaluated using quantitative data from prototype testing and qualitative data from literature, interviews, and case studies that are submitted to statistical analysis with the purpose of identifying common patterns and insights [28]. In order to gauge the proposed framework's efficacy, it is also compared to current security solutions.

To sum up, this technique is designed to build a solid security framework that has been proven by empirical means. It also guarantees that the framework is based on both theoretical knowledge and practical experience. Data integrity, confidentiality, and compliance with regulatory requirements are ensured, addressing the important need for increased security in cloud-based e-health record systems.

IV. PROPOSED FRAMEWORK

Enhancing the security of E-Health Records in cloud settings is recommended via the use of a Cloud-Based Multi-Layer Security Framework, which addresses the intricate problems of data protection, privacy, and compliance. This framework's design is hierarchical, with many levels that address different facets of security. At the base is the Data Layer, where e-health records are securely stored, followed by an Encryption Layer that ensures all data is encrypted both at rest and in transit. Above this is the Access Control Layer, which manages authentication and authorization processes using advanced models like RBAC and ABAC, supplemented by multi-factor authentication for added security.

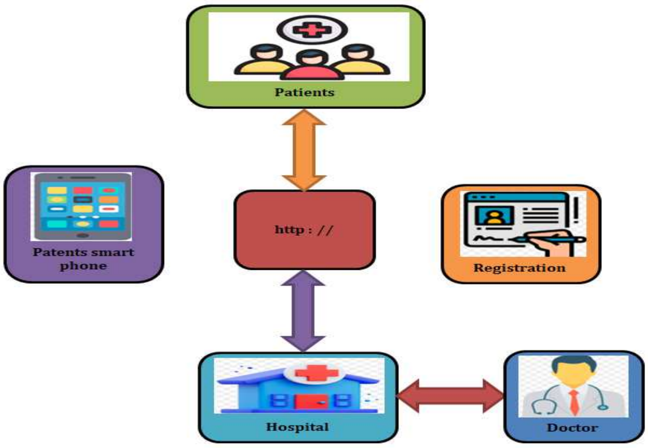

Figure.5: *Steps for Initial Requirement Identification*

Technology and its infrastructure have become integral components of numerous applications in our daily lives. One such application involves the implementation of a strategic approach within the healthcare sector, particularly in hospitals.

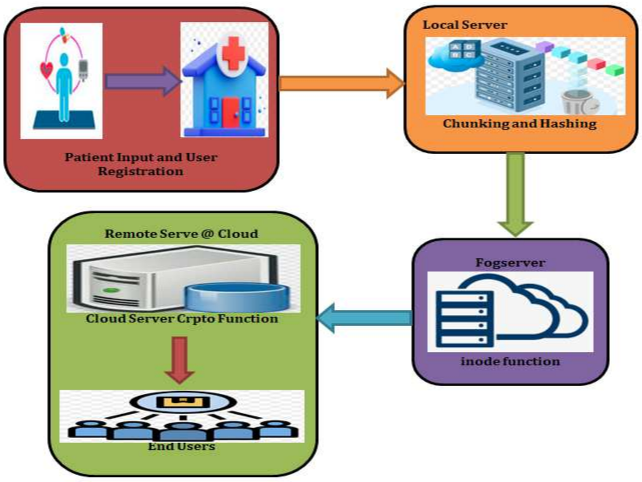

Figure.6: *Cloud Infrastructure for Healthcare Data Storage*

This initiative involves various stakeholders, including patients, healthcare facilities, medical practitioners, nursing staff, administrators, IT professionals, and third-party vendors, often cloud service providers. The process commences with patient/user registration through a portal, mobile application, or in-person interaction, as depicted in Figure.5. Upon registration, the system generates a unique patient ID. Subsequently, the patient enters their health-related issues on their dedicated patient sheet or column. Based on the reported concerns, the system then assigns an appropriate doctor, considering the patient's preferred date. Once the patient confirms the appointment, the process advances to the doctor's delegation stage. Patient information, the initial medical assessment of patients, and their health concerns are all regularly updated in the patient's medical history. When a patient has an appointment with a doctor, the doctor is granted privileges to access and review the patient's complete medical history. Access permissions for hospital administrators, doctors, nurses, and other staff members are managed separately through a designated vendor. Subsequently, the doctor may recommend various diagnostic tests, scans, X-rays, or prescribe medications based on the patient's reported symptoms, and these recommendations are documented along with relevant reports in the patient's medical history. The comprehensive framework for e-health cloud storage is illustrated in Figure 6. A critical component of the framework is the Monitoring Layer, tasked with continuous surveillance of the system to detect and mitigate threats in real-time. This layer makes use of sophisticated intrusion detection and prevention technologies. The Application Layer, situated atop the Monitoring Layer, has underlying layers that put rigorous restrictions on healthcare applications' access to the stored data. At the very top of the system, the Compliance Layer is responsible for ensuring compliance with all applicable laws and regulations, such as GDPR and HIPAA. This system's architecture makes it appropriate for use in a variety of real-world healthcare environments. This approach, which includes cloud security measures, healthcare staff training and awareness campaigns, and connectivity with current healthcare IT systems, requires coordination with Cloud Service Providers (CSPs). The scalability of the system may be advantageous to healthcare organizations of various sizes and data volumes. As technology advances and new cyberthreats emerge, the framework's efficacy is maintained by ongoing review and adjustment. Our multi-layered approach to healthcare data security strives to tackle present and future dangers by providing secure cloud-based electronic health record solutions in an easily scalable way.

V. EVALUATION

A comprehensive battery of tests and analyses was used to assess the efficacy and efficiency of the Cloud-Based Multi-Layer Security Framework for Protecting E-Health Records. Thorough penetration testing, which simulated several cyberattacks to assess the framework's resistance to possible security breaches, served as the foundation for the study. We also investigated the system's general functionality and responsiveness in order to have a better understanding of how the security layers affected performance.

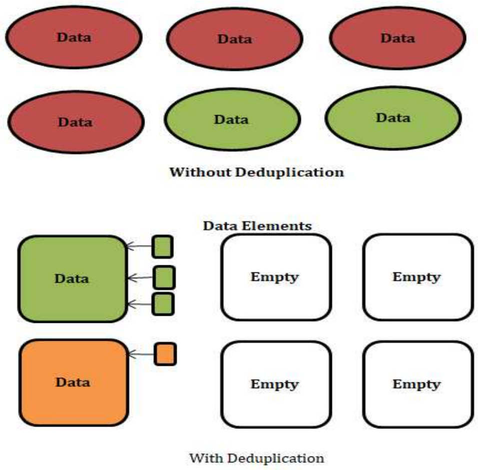

Figure.7: *Pre and Post Deduplication Comparison*

Compliance testing was required to make sure the framework conforms with significant legislation like HIPAA and GDPR. The results of data deduplication both before and after deployment are shown graphically in Figure 7. During this process, redundant data pieces are removed from storage, leaving only unique data components for potential future retrieval. As can be seen in the image, only two separate components remain after data deduplication, out of six data items in the beginning. The company was able to make significant savings on storage solutions as a result of the sharp decrease in data redundancy.

User Acceptance Testing (UAT) was used to ascertain the framework's viability and utility by having actual healthcare professionals utilize the system and provide input on how it would function in a real-life scenario. Stress testing was also used to evaluate the framework's resistance to distributed denial-of-service (DDoS) attacks and high data traffic. These assessments produced encouraging findings. Ensuring data security and privacy, the architecture has shown a strong resistance to several cyber-attacks. Performance testing showed a little increase in the system's capacity to maintain optimum throughput and reaction time, both of which are indicators of strong data processing capabilities. Following receipt of the compliance test findings, the framework was deemed to be fully compliant with all relevant legal and ethical requirements. The majority of UAT responses were favorable. Healthcare professionals praised the system's usefulness and security aspects. Large data loads and hostile assaults were met with the architecture's amazing resilience. The single-layer security mechanisms used by all current security systems are surpassed by the suggested multi-layer technique. Its comprehensive design ensured a greater degree of security by offering improved resistance against a range of cyber threats. Scalability was a key component of the system since it allowed it to handle growing data loads without noticeably degrading performance. Its high degree of user acceptability suggests that it might be a suitable match for implementation in actual healthcare settings, especially when contrasted to earlier and more sophisticated systems. More evidence that the framework is superior to many existing e-health record security solutions is its capacity to withstand stressful situations while preserving data availability and integrity.

VI. RESULTS AND DISCUSSION

The evaluation's findings may provide insight into the potential advantages and effects on healthcare data security of the Cloud-Based Multi-Layer Security Framework for Protecting E-Health Records.

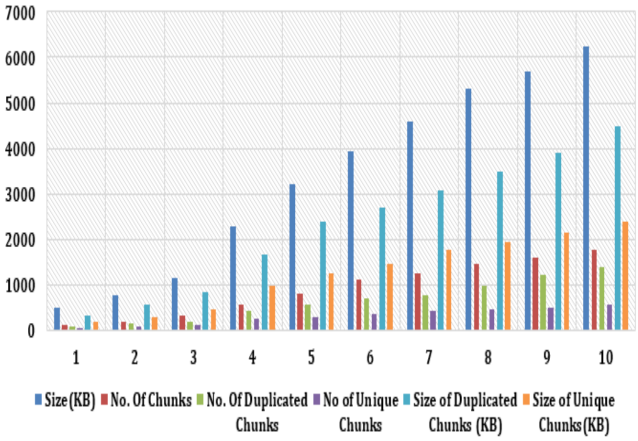

Figure.8: *Metrics for measuring the performance*

The framework's ability to provide a high level of data security is shown by its strong performance against various cyber threats, which is a crucial need in the rapidly digitizing healthcare industry. The endurance of the system, particularly in situations requiring stress testing, demonstrates its dependability. Access control, encryption, and real-time monitoring are just a few of the many security measures this framework uses. This multifaceted approach enhances the security of electronic health data while mitigating the many potential risks associated with cloud computing. Considering the different capabilities of healthcare providers, it is essential to create a framework that can be easily expanded to accommodate businesses of all sizes.The input data is supplied in different-sized data chunks that are further subdivided. Figure 8 examines the diameters of both unique and similar pieces in detail. The application is tested locally and in the cloud with data volumes varying from very small to very big in order to assess its efficiency in terms of latency and space usage. Among the security concerns raised by adopting the cloud deduplication method is protecting against Man-in-the-Middle attacks and other security vulnerabilities. One significant challenge, especially for smaller healthcare organizations with limited resources, is the intricate implementation of the system. The intricacy of the framework may prevent it from being adopted more widely. Even while the architecture is designed to minimize the impact of the extra security layers on system performance, it is nevertheless vital to consider the possible overhead provided by them in resource-constrained scenarios. With a focus on the prescriptions associated with each patient, we assess the storage costs in the context of 500 patient records. Figure 9 illustrates the cost savings that came about as a consequence of using the ESRD approach. The proposed method dramatically lowers storage expenses after compression and data processing.

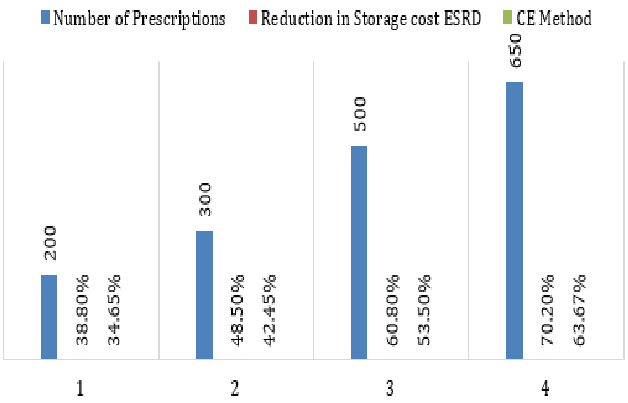

Figure.9: Cost-Efficient Storage Solutions

Additionally, for the framework to function, healthcare workers must adhere to the established security guidelines. This reliance draws attention to the vital need of ongoing education and awareness campaigns, which is something that is sometimes missed in current solutions. In the future, cutting-edge technologies like artificial intelligence (AI) and machine learning (ML) will be included into the framework to further improve threat detection and response protocols. Continuous research and development are also necessary to ensure that the framework can adapt to new technology advancements and changing threat environments. Last but not least, the Cloud-Based Multi-Layer Security Framework is a fantastic advancement in safeguarding cloud-based electronic health data. Numerous problems in the area are currently being resolved by it since it is all-inclusive, scalable, and user-friendly. However, there is still need for additional study and development into this framework due to its complexity and the constant need for adaptation to keep up with the rapidly evolving digital world.

VII. CONCLUSION

A number of noteworthy discoveries that demonstrate how the framework has the ability to completely transform cloud health data security are the culmination of Evidence-Based Practices for Ensuring the Safety of Electronic Health Records in the Cloud. The framework's multi-tiered design successfully prevented a range of cyberattacks, protecting the security and privacy of patients' medical data. A vital element of the dynamic healthcare industry is the capacity to adjust to the needs of healthcare providers of different sizes and skill levels. However, the study indicates that there are problems that need to be addressed. The system's complexity and the ongoing need for upgrades and modifications to address changing cyberthreats and technical advancements are a few of these difficulties. Healthcare firms must regularly carry out educational activities due to the significance of user compliance and training. In the long run, this framework creates the foundation for further in-depth study on the subject in the future. More research might focus on improving system interoperability across platforms, optimizing resource use to avoid performance effect, and figuring out how to merge AI and ML for automated threat response and predictive analytics. This work is significant because it addresses the pressing need for robust, scalable, and user-friendly cloud-based e-health record security solutions. Though it offers a solid basis, the constantly evolving world of healthcare technology and cyber risks demands continued innovation and study in this vital subject.

REFERENCES

1. R. Kishore Kumar, M. Pandidurai and M. S. C. Senthil Kamalesh, (2023) "Design of IoT based Rural Health Helper using Natural Language Processing," 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, pp. 328-333.
2. B. Ram Vishal, M. U. Shankar and K. A. M, (2023) "Cardiovascular Disease Prediction Using LSTM Algorithm based On Cytokines," 2023 4th International Conference for Emerging Technology (INCET), Belgaum, India, pp. 1-5.
3. D. Palanikkumar, P. A. Mary, A. Y. Begum, (2023) "A Novel IoT Framework and Device Architecture for Efficient Smart city Implementation," 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, pp. 420-426.
4. Nareshkumar and B. Gururaj, (2022) "An Integrated IoT Technology for Health and Traffic Monitoring System with Smart Ambulance," 2022 IEEE North Karnataka Subsection

Flagship International Conference (NKCon), Vijaypur, India, pp. 1-6.

5. R. Kavitha, A. Kumar, V. Kalpana and V. Hariram,(2023) "Artificial Intelligence based Health Monitoring System on IoTH platform," 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, pp. 1458-1463.
6. S. Archana Shreee, B. Maheshwari, G. Jeevitha Sai, (2023) "A Novel Method of Identification of Delirium in Patients from Electronic Health Records Using Machine Learning," 2023 World Conference on Communication & Computing (WCONF), RAIPUR, India, 2023, pp. 1-6.
7. M. Kranthi, and R. C. Tanguturi,(2023) "Design of Intelligent Medical Integrity Authentication and Secure Information for Public Cloud in Hospital Administration," 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India, pp. 256-261.
8. R. C. Tanguturi, L. S. V. S. L, S. R. C. K and V. C. H, (2023) "Implementation of Machine Learning Approach for Detecting Cardiovascular Diseases," 2023 3rd International Conference on Intelligent Technologies (CONIT), Hubli, India, pp. 1-6.
9. R. V. Mailapur and M. K, (2023) "Implementation of GUI based Vital Track Ambulance for Patient Health Monitoring," 2023 8th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, pp. 1417-1424.
10. S. Venkatakiran, B. Ashreetha and N. S. Reddy, (2023) "Implementation of a Machine Learning-based Model for Cardiovascular Disease Post Exposure prophylaxis," 2023 International Conference for Advancement in Technology (ICONAT), Goa, India, pp. 1-5.
11. Sadashiva V. Chakrasali, Chanakya Kumar, Abhay Chaturvedi, A. Azhagu Jaisudhan Pazhani, (2023) Computer vision based healthcare system for identification of diabetes & its types using AI, Measurement: Sensors, Volume 27, 10075.
12. Hombalimath, D. Palanikkumar, and N. Patwari, (2023) “Symmetrized Feature Selection with Stacked Generalization based Machine Learning Algorithm for the Early Diagnosis of Chronic Diseases,” 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, pp. 838-844.
13. Namitha A R, Manu Y M, Rashmi G R and Veera Sivakumar Chinamuttevi (2022), IOT Based Smart Health Care System to Monitor Covid-19 Patients. IJEER, 10(1), pp.36-40.
14. P. Ramesh Naidu and N. Guruprasad (2021), A High-Availability and Integrity Layer for Cloud Storage, Cloud Computing Security: From Single to Multi-Clouds, Journal of Physics: Conference Series, 1921 (1), pp. 012072.
15. G. A, A. B. Naik and N. HG, (2021) "Covid-19 Prevention Kit Based on an Infrared Touchless Thermometer and Distance Detector," 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 358-362.
16. K. Jeevan and B. M. Sathisha, (2020) "Implementation of IoT Based Wireless Electronic Stethoscope," 2020 Third International Conference on Multimedia Processing, Communication & Information Technology (MPCIT), pp. 103-106.
17. U. K N and R. V M, (2022) “Arduino based COVID-19 Suspect Detection Device,” 2022 6th International Conference on Electronics, Communication and Aerospace Technology, Coimbatore, India, pp. 158-163.
18. M. R. G. and H. Anandaram, (2022) “Extraction of Fetal ECG Using ANFIS and the Undecimated-Wavelet Transform,” 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT), pp. 1-5.
19. Revanna C R, B. Kameswara Rao and Parismita Sarma (2022), Enhanced Diagnostic Methods for Identifying Anomalies in Imaging of Skin Lesions. IJEER 10(4), pp.1077-1085.
20. S. Reddy P, P. S. Patwal, (2022) “Data Analytics and Cloud-Based Platform for Internet of Things Applications in Smart Cities,” 2022 International Conference on Industry 4.0 Technology (I4Tech), pp. 1-6.
21. S. R. Kawale, S. P. Diwan, (2022) “Intelligent Breast Abnormality Framework for Detection and Evaluation of Breast Abnormal Parameters,” 2022 International Conference on Edge Computing and Applications (ICECAA), pp. 1503-1508.
22. B. Kameswara Rao, Abhay Chaturvedi, Naziya Hussain, (2022) Industrial quality healthcare services using Internet of Things and fog computing approach, Measurement: Sensors, Volume 24, 100517.
23. M. Swathi Pai, M. Shruthi and B. Naveen K, (2020) "Internet of Things: A Survey on Devices, Ecosystem, Components and Communication Protocols," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 611-616.
24. K. B. Naveen, M. Ramesha, and G. N. Pai,(2020) “Internet of things: Internet revolution, impact, technology road map and features,” Adv. Math. Sci. J., vol. 9, no. 7, pp. 4405–4414.
25. P. Ramesh Naidu, N. Guruprasad, (2020) “Design and implementation of cryptcloud system for securing files in cloud,” Adv. Math. Sci. J., vol. 9, no. 7, pp. 4485–4493.
26. K. Prasad, S. Dekka, R. c. Tanguturi and G. Poornima, (2022) "An Intelligent System for Remote Monitoring of Patients Health and the Early Detection of Coronary Artery Disease," 2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, pp. 1-6.
27. H. Anandaram, N. B. A, N. Gupta and B. K. Verma, (2023) "IoT Wearable Breast Temperature Assessment System," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, pp. 1236-1241.
28. K. Prasad, N. Anil Kumar, N. S. Reddy and B. Ashreetha, (2023) "Technologies for Comprehensive Information Security in the IoT," 2023 International Conference for Advancement in Technology (ICONAT), Goa, India, pp. 1-5.