International Journal of Linguistics Applied Psychology and Technology
https://ijlapt.strjournals.com/index.php/ijlapt
vol. 01 issue 01 (2024)
ISSN: 3048-4529

SECURE DECISION SUPPORT SYSTEM IN MEDICAL CYBER PHYSICAL NETWORK

Sharad Chandra Acharya[1], Mr. Sabir Ali[2]

[1,2]Department of Digital Communication

Marudhar Engineering College, Bikaner Technical University

Abstract

Medical Secure Systems (MSSs) represent a fusion of computational and physical processes, posing significant challenges in both theory and application. This study aims to delve into this burgeoning multidisciplinary approach, particularly focusing on MSS within medical contexts, commonly referred to as Medical Secure Systems (MSS). Within MSS, the transmission of diverse data to either private or public cloud platforms for storage and analysis is commonplace. Leveraging machine learning algorithms, these data sets can be processed to facilitate informed decision-making by healthcare professionals. However, the sensitivity of such data, coupled with its exposure to third-party storage spaces, underscores the criticality of security measures. To address these concerns, this paper employs cryptographic techniques, notably AES encryption, to safeguard data before its storage on cloud servers. Moreover, an additional layer of security is introduced through the implementation of digital envelopes. Here, the AES encryption key is further encrypted using ECC encryption, bolstering the overall security framework. Furthermore, to streamline key management, the system utilizes a Key Distribution Center (KDC), tasked with generating and managing keys for all users. Experimental findings validate the efficacy of this MSS system, affirming its superior security posture compared to previous iterations while also minimizing key management overhead.

Keywords:- *Medical Secure Systems, Key Distribution Center, AES, encryption, security.*

I. INTRODUCTION

The confluence of technology and healthcare in recent years has sparked a revolutionary movement that goes much beyond traditional medical procedures. Leading this paradigm change is the rapidly developing field of Medical Secure Systems (MSS), a dynamic, multidisciplinary discipline that combines computation, control, and communication to completely reimagine healthcare delivery. Because of the significant effects this research will have on the environment, the economy, and society, government agencies, business, and academia will all be paying close attention to it.

Despite its official definition being a work in progress, Medical Secure Systems are widely recognized as the next generation of designed systems. In the healthcare industry, these systems combine communication, computing, and control to accomplish broad objectives

including reliability, efficiency, resilience, and performance. As impressive as the progress has been in achieving these goals, there is still a concerning omission in the area of security in MSS. The potential ramifications of security breaches are enormous and have the potential to have disastrous effects as these technologies are linked more and more into vital infrastructures.

Take the incorporation of Medical Secure Systems into the rapidly developing field of driverless vehicles, for example. Inaccurate distance information resulting from a breach in the vehicle-to-vehicle communication network may cause accidents. The introduction of autonomous vehicles has made this problem worse since passengers now have to rely on the cars to decide what is safe for them. The unstoppable advancement in these technologies has made it possible to create comprehensive patient health monitoring systems that may be used in clinical settings. These systems use distributed sensor networks to collect patient medical data, which is then sent to cloud services via statistical inference algorithms to identify patterns with established illness states. These frameworks, known as Medical Secure Systems (MSS), represent a new chapter in the history of Digital Health (D-Health) and provide hitherto unheard-of difficulties in protecting health data while it is being transmitted.

Information aggregation, cloud management, activity, AES encryption, Key Distribution Center, and Digital Envelope are all included in the seven-layer structure of the Medical Secure System, and each is essential to maintaining the security and integrity of private health data. The effective construction of MSS depends critically on overcoming the mechanical challenges involved in constructing these structural elements, which include sensors, cloud computing structures, high-speed internet, and mobile phone connections.

II. LITERATURE SURVEY

Any new research endeavor must begin with an assessment of what is currently known and build upon the comprehension gained from past investigations. In the context of Medical Secure Systems (MSS) and cryptographic approaches, it is vital to conduct a comprehensive literature analysis in order to understand the evolution of these domains, identify gaps, and contextualize the research that is currently being conducted.

The progression of Medical Secure Systems has been characterized by a dynamic interplay between the expanding needs of the healthcare sector and technological advancements. This relationship has been the driving force behind the growth of Medical Secure Systems. The earliest initiatives in the field of medical informatics focused mostly on the storage of fundamental data as well as electronic health records (EHRs). However, the use of technology in medical processes is increasing, which results in the development of more complicated systems, such as MSS. The pioneering work done by academics such as [1] and [2] laid the groundwork for a better understanding of the challenges posed by the convergence of medical data and security systems. This laid the framework for understanding the difficulties posed by the convergence of security systems and medical data. One important tendency that has been identified in the aforementioned body of research is the shift toward distributed architectures. It was found out that conventional centralized methods

were susceptible to security flaws as well as single points of failure. The distributed multi-level security system (MSS), which was proposed by [3] and [4], ushers in a paradigm shift by decentralizing data and computation among multiple nodes, thereby simultaneously enhancing operational efficacy and data safety.

Even if the use of cryptographic methods to healthcare systems is not a novel concept, current advancements have rendered it more pertinent than it has ever been before. To be more specific, encryption has evolved into an essential part of the process of protecting medical data. The efficacy of encryption methods in ensuring the confidentiality of patient medical records has been demonstrated by a number of prominent investigations, including those carried out by [5] and [6]. In addition, the literature investigates the challenges that are faced by key managers in healthcare systems. By underlining the significance of efficient key distribution systems, the work of [7] sets the foundation for the integration of Key Distribution Centers (KDC) in MSS.

III. PROPOSED METHODOLOGY

Detailed descriptions of the proposed system are as follows:

Users can peruse the input dataset, which is essential for applications related to medicine. The sections that follow provide more dataset specifics.

a. Data Preprocessing: A training file is created for classification algorithms as part of the preprocessing of the dataset.
b. Data Encryption: The system uses AES encryption to encrypt data in order to protect it from potential attacks.
c. Classification: Classifying patient data is a necessary part of operating a decision support system. This is done by the SVM classifier on the server, and the findings are sent to medical specialists so they may decrypt the data.
d. Key Distribution Center (KDC): Digital envelope and integrity checks are carried out by KDC and Third-Party Authentication (TPA). To improve data security, KDC creates master keys, public-private key pairs, and encrypts the master key using an ECC public key.

International Journal of Linguistics Applied Psychology and Technology
https://ijlapt.strjournals.com/index.php/ijlapt
vol. 01 issue 01 (2024)
ISSN: 3048-4529

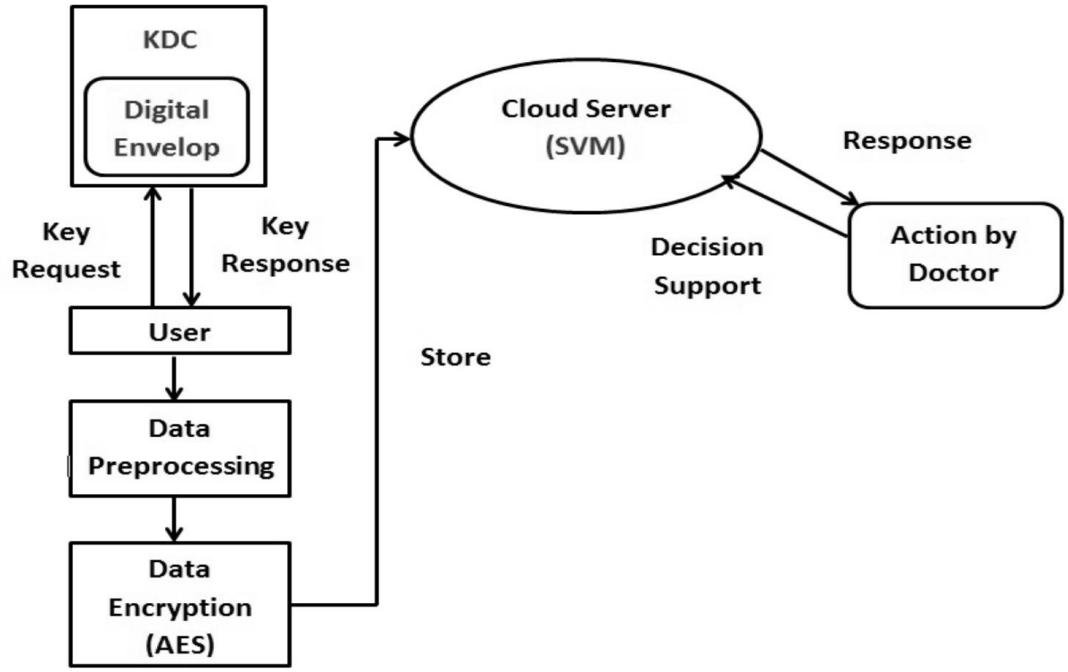

Fig 1. System Architecture

IV. RESULTS

Based on the domain of the system, the comparison analysis shows better performance than current systems in terms of time and memory. The incorporation of context, which gives the key created for encrypted files a digital envelope, is a crucial differentiator. Time and memory measurements are the main focus of the analysis.

The time comparison graph between the suggested system and the current system is shown graphically in Figure 1. The graph shows that implementing the system with KDC takes less time than implementing it without it. Time is expressed in milliseconds here. The current system needs between 500 and 550 kb, whereas the suggested system, which uses KDC, only 50 kb.

The memory comparison graph between the suggested system and the current system is shown in Figure 2. The graph shows that the KDC-equipped system uses less memory than the non-KDC system. The framework output of the proposed system during the phase of result analysis is shown in the graph. It displays the total amount of RAM that can be needed, showing a significant gap between the current system's 28000000kb requirement and KDC's 10000000kb.

A comparison of the storage memory needed for the training file and the dataset is shown in the last figure, 3. The graph highlights the fact that the dataset file requires more memory than the training file.

International Journal of Linguistics Applied Psychology and Technology
https://ijlapt.strjournals.com/index.php/ijlapt
vol. 01 issue 01 (2024)
ISSN: 3048-4529

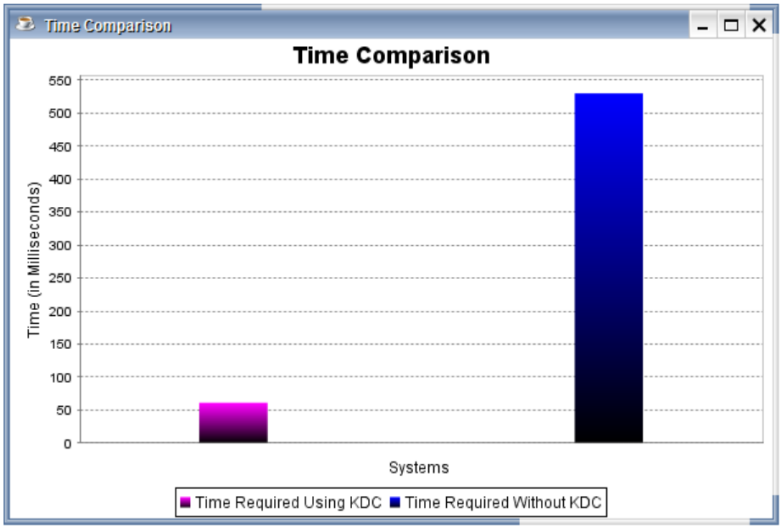

Fig. 1. Time Comparison

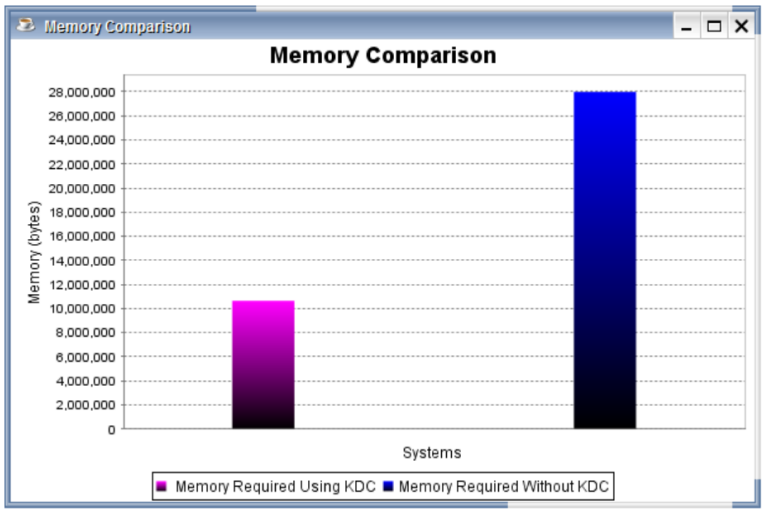

Fig. 2. Memory Comparison

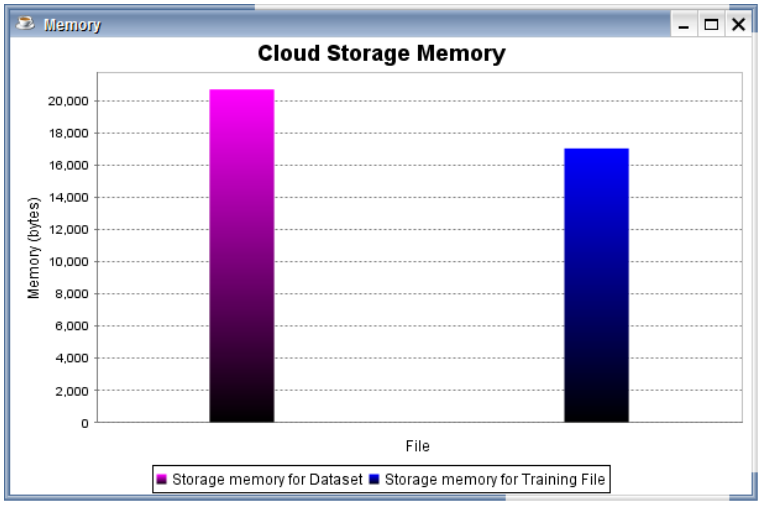

Figure 3 Cloud Storage Memory

V. CONCLUSION

In summary, the investigation of the suggested Medical Secure System (MSS) has revealed a future in which the fusion of technology and healthcare serves as a guiding light. The research's overall conclusions and contributions provide a clear picture of a reliable, safe, and effective system that has the potential to completely transform the nexus between technological advancement and medical research. This work's main goal was to solve a vital yet sometimes disregarded security issue with medical secure systems. Resilient and secure systems are becoming more and more important as medical devices advance and incorporate embedded software and network connectivity.

The MSS's seven-layered architecture, which includes digital envelopes, data gathering, encryption, and key management, offers a thorough answer to the security issues raised by the integration of medical systems with vital infrastructures. By comparing the suggested system with the current one, the comparative analysis revealed the concrete advantages of implementing the Key Distribution Center (KDC). Time and memory metrics both demonstrated notable gains, highlighting the effectiveness and resource optimization attained by the creative integration of KDC. The dynamic and time-sensitive field of healthcare is one where the decrease of execution time and economical memory footprint are especially important. The investigation of cloud storage issues revealed complex information about the amount of memory needed for various kinds of data.

REFERENCES

1. OvuncKocabas, TolgaSoyata, and Mehmet K. Aktas, “Emerging Security Mechanisms forMedical Cyber Physical Systems”, IEEE/ACM transactions on computational biology andbio-informatics, vol. 13, no. 3, may/june2016.
2. Phaneendra Kumar, Dr.S.V.A.V.Prasad ,ArvindPatak, “Design and Implementation of MHealthSystem by Using Cloud Computing”, Future Gener. Comput.Syst.,Vol. 5, Issue 5,May 2016.
3. Tran Viet Xuan Phuong, Guomin Yang, Member, IEEE, and Willy Susilo, Senior Member,IEEE, “Hid-den Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions”,IEEE transactions on information forensics and security, vol. 11, no. 1, January 2016.
4. Abdelghani Benharref and Mohamed Adel Serhani, “Novel Cloud and SOA-Based Framework forE-Health Monitoring Using Wireless Biosensors”, IEEE journal of biomedical and health informatics, vol. 18, no. 1, January 2014.
5. OvuncKocabas, TolgaSoyata, “Utilizing Homomorphic Encryption to Implement Secure and Private Medical Cloud Computing”, 2015 IEEE 8th International Conference on Cloud Computing.
6. X. Yao, Z. Chen, and Y. Tian, “A lightweight attribute-based encryption scheme for the internet of things”, Future Gener.Comput.Syst., vol. 49, pp. 104-112, 2015.
7. O. Kocabas and T. Soyata, “Towards privacy-preserving medical cloud computing using homomorphic encryption”, in Enabling Real-Time Mobile Cloud Computing through Emerging Technologies, T. Soyata, Ed. Hershey, PA, USA: IGI Global, 2015, ch. 7, pp. 213-246.

8. J. A. Akinyele, C. Garman, I. Miers, M.W. Pagano, M. Rushanan, M. Green, and A. D. Rubin,“Charm: A framework for rapidly prototyping crypto systems”,J. Cryptographic Eng., vol.3, no. 2, pp. 111-128, 2013.
9. Robert Mitchell, Ing-Ray Chen, Member, IEEE, “Behavior Rule Specification-based Intrusion Detection for Safety Critical Medical Cyber Physical Systems”,Robert Mitchell,Ing-Ray Chen, Member, IEEE, 2013.
10. Alhassan Khedr, Member, IEEE, and Glenn Gulak, Senior Member, IEEE, “SecureMed: Secure Medi-cal Computation using GPU-Accelerated Homomorphic Encryption Scheme”,2016.
11. P. Khan, Y. Khan and S. Kumar, "Tracking and Stabilization of Heart-Rate using Pacemaker with FOF-PID Controller in Secured Medical Cyber-Physical System," 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), 2020, pp. 658-661, doi: 10.1109/COMSNETS48256.2020.9027302.