Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 21s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

A Centralized E-Health Medical Records Security Using aes Technology

Atmakuri Sowjanya[1], Moulana Mohammed[2]

[1]PG Student, CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur.

Email ID: gugiatmakuri@gmail.com

[2]Professor, CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur.

Email ID: moulanaphd@gmail.com

Cite this paper as: Atmakuri Sowjanya, Moulana Mohammed, (2025). A Centralized E-Health Medical Records Security Using aes Technology. *Journal of Neonatal Surgery*, 14 (21s), 587-595.

ABSTRACT

In this research work an adaptive centralized E-health management system and its security are initialized using MySQL based PowerBi platform. Medical records monitoring as well as its security has been important to future generations. The centralized storage system is playing a key role in this contest, moreover proposed model has been implemented using AES technology. Medical records sharing is very important for clients, users, doctors and third parties but when sharing documents there may be a chance to get hack significant information. In this study using AES algorithm has been providing security to medical records using encryption and decryption (via key). The centralized dashboard, nothing but patients and doctor's dashboard is maintained by designed application using MySQL based PowerBi tool. This application provides performance measures in terms of accuracy 98.34%, sensitivity 94.35%, recall 93.23%, encryption rate 76.34% and decryption rate 75.34& had been attained which have been outperforming the methodology and compete with present technology

Keywords: E-health, centralized medical application, AES, security

1. INTRODUCTION

Most hospitals now keep an electronic medical record since the patient medical record is the primary source of information about the patient's treatment. When proof is needed to defend the service provider on patient care, the medical record comes in handy. The fundamental issue with current record management is that all records are maintained in a centralised manner, meaning that all data is kept in one place. In such centralised storage systems, an intruder or a third party has a significant chance of accessing and changing the data. In this study, we propose a website-based method to address this issue. In the country's health-care system, the EHealth Application is critical. When compared to a manual system, E-Health meets the needs of consumers' health problems everywhere, anytime, and at any age via a broad variety of e-health solutions. It also allows for remote access to certain data. This model features a front-end made of HTML and CSS, as well as a middle-end made of PHP and MYSQL connection. EHealth was designed specifically to fulfil the needs of mid- and large-sized hospitals throughout the world. The application's solid database makes it more user-friendly and extensible. It includes all essential modules, such as Patient Registration, Doctor, Admin, Patient Appointment, Record Modification, and so on. To construct such a system, security techniques such as two-factor authentication and data encryption are required. It uses PowerBi to generate patient registration data for the sake of analysing and implementing new procedures.Wireless and Micro-Electro-Mechanical System (MEMS) sensor nodes are now possible because of recent advancements in medical sensors and wireless technology. Wireless sensor networks (WSNs) based on these lightweight, tiny nodes make it easier to monitor patients' health. Thanks to this new technology, remote patient surveillance may be provided in both hospital and non-hospital settings. As a result, healthcare costs are reduced, and patients' quality of life and treatment outcomes are improved.

Medical WSN for patient surveillance has been the subject of several studies [1]. The BAN is a collection of sensors that patients wear to monitor their health. Receives the gathered data via a wireless communication channel (ADSL, WiFi, 3G, or satellite). Keeping, processing, and accessing all of the data is done in one place.

Medical devices are sampled at a rapid rate, increasing the quantity of data that may be gathered. In addition, if a patient's condition worsens, the frequency of sensor sampling may be increased. Demand for more storage space and processing power is driven by data growth and heterogeneity. People also must think about how well the system can grow. Medical data could save lives, so it must always be available and from any place. Current systems, which store, and analyses sensed data using a centralized paradigm, cannot address the problems listed above. Sensor data is growing at an exponential pace, and we must find new and creative ways to deal with it.

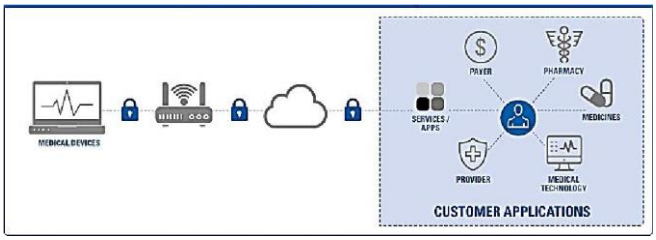

Figure :1 Medical records security system

To ensure patient privacy, only those with a legitimate need for the data should have access shown in figure 1. Medical diagnosis relies heavily on the integrity of data, so it's important to ensure that information isn't tampered with in a hateful or mistaken way. Access to medical data is generally regulated by sophisticated regulations that differentiate between each piece of information and individual user's access rights. Admittance control at the finegrained level required to enable dynamic and sophisticated organizational rules is thus a difficult task to accomplish. Practical issues, such as how much time it takes to manage security, how much money it costs, and how well access control can grow as the number of users grows, are also important. Many studies have been done in the field of medical wireless sensor networks, but security has yet to be addressed in any significant way [2].

In this study, we look at how to manage data in wireless sensor networks that are used to keep track of patients. Medical sensor networks create enormous amounts of data, which must be collected and accessed securely and quickly. Storage resources may be provisioned on-demand using cloud computing technologies. There are several ways in which we've contributed to this project: As a starting point, we suggest entirely new medical wireless sensor network architecture based on the cloud. The third thing, I suggest is a new approach to access control that makes it possible to implement the dynamic and complicated security rules required for medical applications while also lowering the administrative and processing burden. It's all about combining CPABE with symmetric encryption in order to get fine-grained access with the least amount of work.

II. LITERATURE SURVEY

Eldefrawy, M. H., Alghathbar, K., et al [2011] Since users must supply both something they know and something they have in order to utilise two-factor authentication (2FA), it increases security. This technique provides a greater degree of authentication and certainty, which is critical for the safety of online banking. This model also lowers the limits imposed by the SMSc system.[1] Kahani, N.,et al [2016] The ability to access unlimited computed and storage resources on demand has prompted customers to shift their health information from local data centres to the cloud. This adjustment may minimize data management and transmission expenses while improving service quality (QoS). To persuade people to migrate sensitive medical information to the cloud, rigorous authentication and access control must be implemented. We present a novel mechanism for e-Health data access that retains both verification and admission switch. It assesses our scheme's data secrecy and network attack resistance. The suggested solution can handle a lot of simultaneous authentication requests while still giving a good response time.[2] Thimmaiah, C. D.,et al [2019] Hospitals and health systems still face significant problems in installing, maintaining, and updating EHR systems. This article examines the challenges that arise while using EHRs and potential solutions. In order to maintain a single version of the truth and protect health information, blockchain may be a possible option. Doctors, hospitals, labs, and other health insurers might seek access to a patient's data to record transactions and suit their purposes. Using the blockchain to construct a distributed access and validation mechanism may assist in totally replacing the present centralised middlemen. Thus, addressing today's health record issues.[3] Shrestha, N. M.,et al [2016] In an increasingly popular patient-centric paradigm, PHRs are typically stored by third parties. This protects health information from unauthorized users. This study proposes new, secure e-health architecture. Personal health information is protected by digital signatures and patient faux identities. This research aims to uncover a novel approach used to construct an e –healthcare. Chenthara, S.,et al [2019] A systematic and thorough evaluation revealed that many privacy-preserving techniques exist privacy. Studies must concentrate on efficient and complete EHR security procedures and approaches to ensure patient data integrity and confidentiality. [5] Sharma, Y., et al [2020] Electronic health records (EHRs) are patient health records stored digitally on a network. EHRs provide several potential improvements to patient care, clinical practice, and future clinical research. In the age of smart cities and homes, the methods employed to store EHRs are particularly insecure. Hackers and unauthorized third parties may readily access the data. Blockchain technology offers an immutable ledger system that allows for decentralized transactions. Securing, decentralizing, and transparency are the three key advantages of blockchain technology that keep unwanted parties out. Data tampering is almost impossible on a blockchain network. Using block chain technology, this project proposes a mechanism for securing private EHRs. Using cryptography and decentralization, blockchain technology will govern information access. It will also keep data privacy and data accessibility in check. In this project, the main goal is to think about privacy and security issues in electronic health.[6] These

are paired with a patient-friendly interest and a patient-friendly conscience about their treatment. A lot of medical data is generated. All of these data sets need safe transport. We suggest a very successful encrypty system to maintain the identity privacy of healthcare data. We also considered a multi-level authorization architecture. Access to medical records is often granted to numerous parties. In this work, we used the AT&T system to manage patient data access control. Encryption is done via ARCANA, which offers hierarchical access to data resources. Its access control architecture is based on the XACML access model. Encrypting medical data using multiple permission approaches was also essential for data access legislation. This may boost consumer confidence in the e-health paradigm and hence large-scale usage.[7] Chiuchisan, I.,et al [2017] Healthcare systems' use of medical services and information systems, which are crucial to the security, confidentiality, and access to personal data of the general public, is a topic of great interest, although it is seldom discussed in literature. Home health care systems for screening and rehabilitation have piqued considerable interest and are viewed as a novel way to combat illness. Information security measures have increased as a result of technological advancements in health care information systems, which have allowed for the transition of in-hospital rehabilitation and monitoring of elderly patients to more sophisticated health care systems. This article provides an overview of the security mechanisms and data transmission security involved in health care systems in order to secure patient information. This study focuses on the unique security concerns that must be addressed as a healthcare system is developed for Parkinson's disease patients.[8] Sonya, A., et al [2021] the healthcare industry must address significant difficulties, such as addressing security risks associated with providing healthcare services. Personal data such as demographics and medical histories is stored in EHRs. A novel cryptographic method is proposed to overcome the AES, RSA, and ABS flaws. It is faster, more accurate, and more efficient than the existing three cryptographic methods. The suggested technique significantly improves the security of healthcare records.[9] Lee, Y. L., et al [2022] Clinical data exchange and application in the medical field have had a significant impact. Realizing these three aims will allow hospitals to make patient records more widely accessible, allowing for more comprehensive medical treatment. Cross-agency data interchange necessitates comprehensive definitions and use restrictions for the security and privacy of health data. In this study, there are three major modules. Secured Encrypted Medical Records are a product of the "Combined Encryption and Decryption Architecture," which uses AES and RSA to create hybrid double encryption. Abhishek, B., et al [2022] nowadays, we live in a world entirely dependent on machines. Overall, machines have decreased the amount of manual work and made our lives easier at the same time. When it comes to health care, you don't have to wait in huge lines to receive an appointment or a report. With just a single touch, everything is at your fingertips. Medical data from thousands of hospitals may be compared by physicians using computers or the cloud. Security and privacy are compromised when outsiders get access to sensitive data. Using the Modified Blowfish Algorithm, this research aims to keep patient data safe and secure while it is kept on a variety of devices. With this technique, 72 percent of the time is spent encrypting and 48 percent is spent decrypting information.[11] Sharmin, S., et al [2022] EHR data breaches raise serious privacy and security issues for many healthcare businesses. The existing cryptographic methods used to protect EHR data on the cloud are insufficient. The medical block chain provides interoperability, traceability, and anonymity of patient EHR data. The secure cloud-based medical records blockchain shows patient data in a shared and immutable way.[12] Hussein, H. M., et al [2021] the rapid use of blockchain technology in healthcare huge influence on the sector. The trend of block chain technology healthcare an identified using bibliometric data distribution, venues, keywords, and citations. The security and privacy telecare medical information systems and E-health were also investigated. Gabriel, S. J., et al [2021] the most important information is protected via blockchain, which is the most popular method of security. All transactions made with the use of blockchain technology have a shared, immutable, and transparent history thanks to Blockchain. The adoption of block chain technology ensures security integrity data. The data is encrypted using the AES method. When patients and doctors can talk about a wide range of things, this paper wants to help. It also wants to give patients control over their clinical data so that they can share their data with any medical network in a clear and understandable way, if necessary.[14] Boumezbeur, I., et al [2022] Healthcare organizations should priorities the exchange of patient data included in electronic health records (EHRs). Patients' medical records are increasingly being shared across healthcare institutions using a cloud-based electronic health record sharing programmer. Nonetheless, centralizing data in a cloud environment has the potential to jeopardize the confidentiality and safety of patients. Because of its unique characteristics, blockchain should be seen as a potential solution to these problems. This article suggests block chainbased systems securely sharing and controlling access electronic health record maintaining patient privacy. Ensuring that electronic records are preserved securely by setting user access rights is a goal of the proposed EHR blockchain system. Based on time it takes to encrypt and decode the smart contract and the cost of the smart contract, we evaluate the proposal outcomes. EHRs range in size from 128 KB to 128 MB, with encryption and decryption periods correspondingly long. While the 0.0012-second EHR takes the least amount of time to encrypt, the 128-megabyte EHR takes the most time to do so (1.4149 seconds). Thus, performance and security tests show that the method is safe enough to be used in real life.[15].

III. METHODOLOGY

In this section a brief discussion of AES based health records monitorization and security has been provided.

Authentication: We define an authentication target as the device, the resource to which the individual requests access, and an authenticator as the evidence the individual provides to gain access. The user needs to provide the OTP which is sent to

registered mail ID as a twostep authentication in order to login to the system. For example, a doctor should have access to his patients' medical data, but should not be allowed to get information on other doctor's patients without permission.

Data Encryption: All the incoming/outgoing information is encrypted using OpenSSL algorithm which is very important to maintain confidentiality of the patients and Hospital Data.

Escalation mail: Doctor timetables and scheduled appointments allows doctors to plan and browse their timetables. Also allows sharing such information with patients in order to make an appointment. If there is delay in appointment then an escalation mail is sent to the hospital CEO intimidating about the situation.

Archiving: Archival record are primary sources; they are usually unique. Individual archival records are often an PHP technique that can archive data when it reaches the due date(6months).

SMS notification: Whenever admin creates a new patient record, the patient is notified through an SMS. The SMS is sent to the user using fast2sms api. The patient can then login using credentials provided.

Reporting: Healthcare dashboards provide an instant solution to data analysis needs, allowing to convert mass amounts of data into actionable insights. Microsoft Power BI is used to generate the reports which helps hospitals and healthcare organizations to have an outstanding level of clarity and insight into the data which will help to achieve a better understanding of their overall performance and make better informed business decisions.

Description of Algorithms

In security in e-health application for encrypting the data in the database we use open ssl. OpenSSL is a C library that implements the main cryptographic operations like symmetric encryption, public-key encryption, digital signature, hash functions and so on. OpenSSL also implements the famous Secure Socket Layer (SSL) protocol. Secret Key: Secret key encryption algorithms use a single secret key to encrypt and decrypt data. Types of secret key we included is AES Managed.

Public Key: Public-key encryption uses a private key that must be kept secret from unauthorized users and a public key that can be made public to anyone. we used RSA Crypto Service Provider.

Digital Signatures: Public-key algorithms can also be used to form digital signatures. Digital signatures authenticate the identity of a sender (if you trust the sender's public key) and help protect the integrity of data. we used RSACrypto Service Provider. Hash Values: Hash algorithms map binary values of an arbitrary length to smaller binary values of a fixed length, known as hash values. A hash value is a numerical representation of a piece of data. we included HMACSHA1 algorithm.

AES algorithm

Step 1: input infromation into hexa-decimal format

Step 2: load above format into 4x4 state array Step 3: array setup 4x4 state = [[X o to 4 range] [Y 0 to4]]

Block range (512)

If i in range [04]

If j in range [04]

State array[i][j] =range [32*i-04*j-04*[i-j]]

Step 4: byte addition, rows shifting, column mixing, key generation

The above 4 steps can perform the encryption process

Step 5: decryption with cypher text Step 6: output as original message.

The above algorithm is clearly explaining about deep information about AES encryption and decryption process. First, we need to check the version of open ssl. Key pairs: Generate the key pairs using genrsa-out classes pedia.key 2048.It generates RSA private key Extract Public Key: opensslrsa-in tutorials pedia.key -pubout-out tutorials pedia_public.key Advanced Encryption Standard (AES)

.

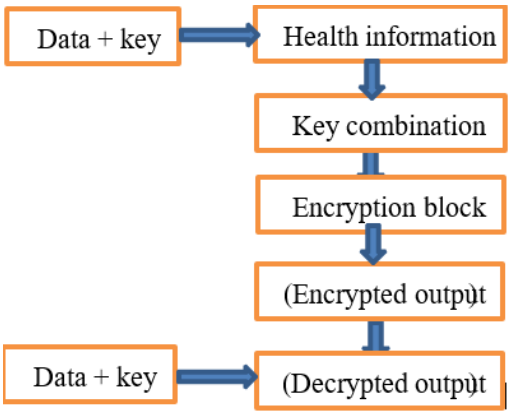

Figure 2: proposed block diagram

In AES algorithm, during the encryption process, each round except the final performs the following four transformations:

Sub Bytes: Operates independently in each byte of the State. Each state byte is replaced with the corresponding Sbox byte.

Shift Row: Rows of the State are shifted in a cyclic manner over different offsets.

Mix Column: Columns of the State considered as polynomials over GF(2^8) are multiplied with a fixed polynomial. This operation is not performed in the last round. iv. Add Round Key: Performs bitwise XOR

Key expansion takes a key of 4-word (16 bytes) as input and produces a44 word (176 bytes) linear array. For the initial Add Round Key stage and every 10 cipher rounds, a 4-word round key is sufficiently provided. The key is copied into the first 4 words of the expanded key. The rest of the expanded key is simultaneously filled in 4 words. Each added word w[i] depends on the immediately preceding word, w[i-1] and the word four positions back, w[i-4].

Byte values in the S-Box are defined as a 16 x 16 matrix which holds the permutation of all possible 8-bit 256 values. The steps performed in mapping each byte of the array to a new byte is as follows: The leftmost 4 bitsof every byte was assumed as row while the leftmost 4 bits were column. The values of these row and column provide indexes into the Sbox to select a unique. Bytes substitution is non-linear which independently operates on every byte using a substitution table. At first, invertible S-box is formed with the values obtained from multiplicative inverse in the finite field GF

(28) with irreducible polynomial m(x) = x8 + x 4+ x3 + x +

1. The element {00} is mapped to itself. Affine transformation is then applied over GF (2).

In the state array, the first row is left unaltered. 1-byte circular left shift is done in the next row. For the third row, a 2- byte circular left shift is performed. For the third row, a 3- byte circular left shift is performed. The rows of the state are shifted in a cyclic manner over different offsets. During decryption, this operation is carried out in the same way except that the values of the shifting offsets are different.

The operation was performed individually on every column. In the column, each byte is mapped to a new value which is the function of all four bytes in the column. This is transformed column-by-column where each column is considered as a four-term polynomial over GF (28) and is multiplication is performed with modulo x 4 + 1.

The 128 bits of the State array and the round key are bitwise XORed which is a column wise operation between the State array and round key.

This is the similar to the encryption process but is simply carried out in reverse order. Here, cipher text block of 128bits is converted to plain text by inversing the four operations. Both the encryption and decryption processes have similar Add Round Key. The three other inverse functions used in this process are Inverse Shift Rows, Inverse Mix-Columns and Inverse Sub Bytes.

2. IV. RESULTS AND DISCUSSION

In this section a brief discussion of designed applications is explained

Parameters	Hit rate	Accuracy	Recall
OTP-based two-factor authentication [1]	28.6	19.7	34.5
Kahani, N [2]	62.8	73.9	56.1
Thimmaiah, C [3]	30.3	17.45	29.1
Shrestha, N [4]	73	58.23	85.6
Chenthara, S [5]	82	74.54	92.34
proposed	94.34	92.74	94.17

Figure 3: results of recall data Figure 3 shows the results by using the above process which we got above mentioned. Also, we got the proposed data results

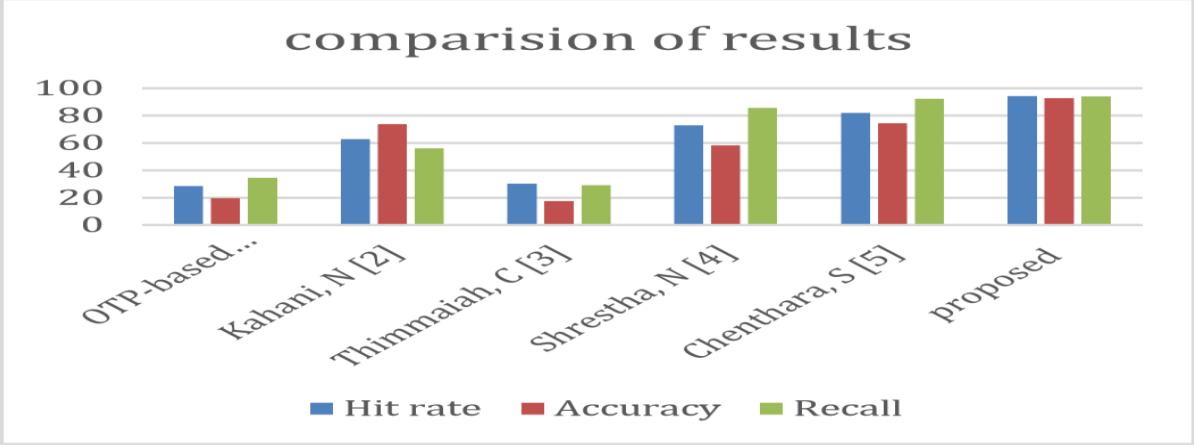

Figure 4: performance estimation

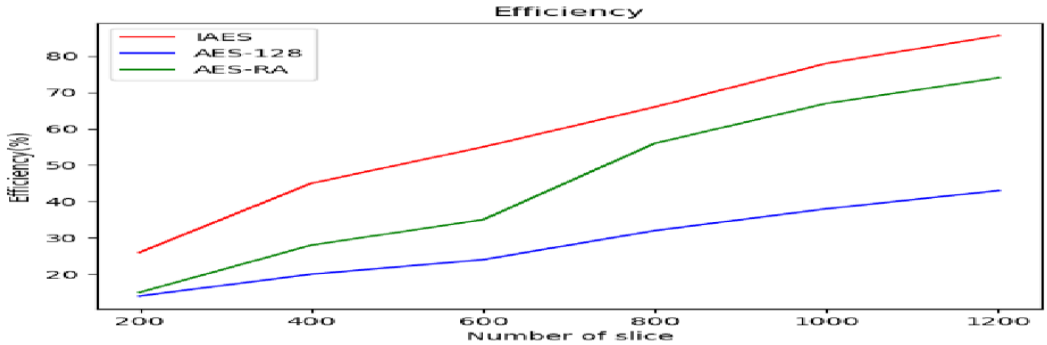

Figure 5: Overall efficiency calculation

Figure 5 shows the analysis of efficiency whereas the proposed IAES achieves 85.6% with the number of slices as 1200. Moreover, the efficiency rate of AES-128 is 43% and AES-RA is 74%. Efficiency is calculated by coinciding with the number of slices in FPGA. Using a smaller number of slices results in better efficiency

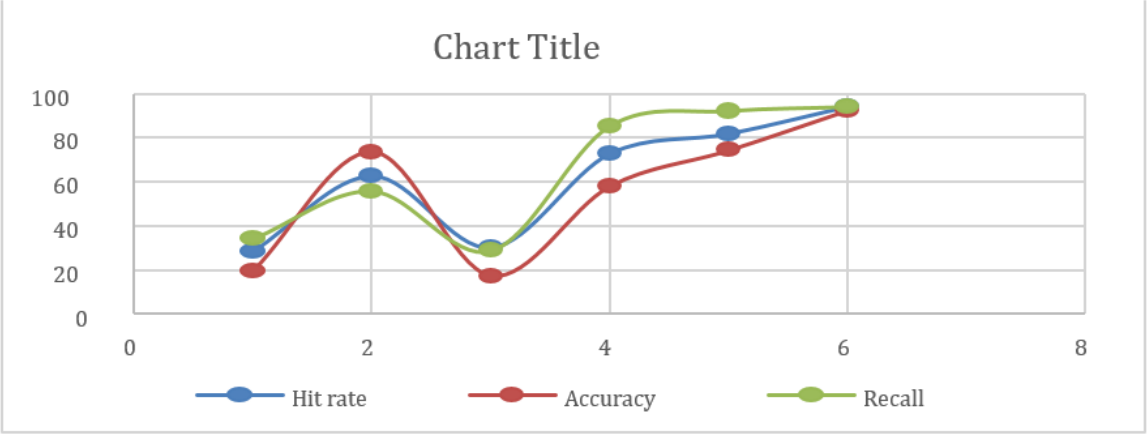

Figure 6: measures estimation

The above figure 6 clearly explains deep analysis on medical health care and security. Here it is noticed that proposed models attain more improvement compared to existing

methods. [15]

3. V.CONCLUSION AND FUTURE SCOPE

In this study, a MySQL-based PowerBi platform is used to [16] set up an adaptive centralised E-health management system and its security. The monitoring of medical records, as well [17] as their protection, is crucial for future generations. In this competition, the centralised storage system plays a crucial role, and the suggested model has been built utilising AES technology. Clients, users, physicians, and third parties all [18] benefit from medical data exchange, but there is a risk of sensitive information being hacked when papers are shared. [19] The AES method was used in this work to provide security to medical records via encryption and decryption (via key). The centralised dashboard, which only shows patients and [20] physicians, is maintained by a specially created application that uses the MySQL-based PowerBi tool. This application has achieved accuracy of 98.34 percent, sensitivity of 94.35 percent, recall of 93.23 percent, encryption rate of 76.34 [21] percent, and decryption rate of 75.34 percent, all of which surpass the approach and compete with current technology

REFERENCES

[1] Eldefrawy, M. H., Alghathbar, K., & Khan, M. K. (2011, April). OTP-based two-factor authentication using mobile phones. In 2011 eighth international conference on information technology: new generations (pp. 327-331). IEEE.

[2] Kahani, N., Elgazzar, K., & Cordy, J. R. (2016, April). Authentication and access control in e-health systems in the cloud. In 2016 IEEE 2nd [23]

[3] international conference on big data security on cloud (BigDataSecurity), IEEE international conference on high performance and smart computing

[4] (HPSC), and IEEE international conference on intelligent data and security

[5] (IDS) (pp. 13-23). IEEE. [24]

[6] Thimmaiah, C. D., Disha, S., Nayak, D., Diya, B. B., & Gururaj, H. L. (2019). Decentralized electronic medical records. International Journal of Research and Analytical Reviews, 6(1), 199-203.

[7] Shrestha, N. M., Alsadoon, A., Prasad, P. W. C., Hourany, L., & Elchouemi, [25] A. (2016, April). Enhanced e-health framework for security and privacy in healthcare system. In 2016 Sixth international conference on digital information processing and communications (ICDIPC) (pp. 75-79). IEEE.

[8] Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud [26] computing. IEEE access, 7, 74361-74382.

[9] Sharma, Y., & Balamurugan, B. (2020). Preserving the privacy of electronic health records using blockchain.

Procedia Computer Science, 173, 171-180. [7] Vora, J., Italiya, P., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., &

[10] Hsiao, K. F. (2018, July). Ensuring privacy and security in e-health records. In 2018 International conference on computer, information and telecommunication systems (CITS) (pp. 1-5). IEEE.

[11] Chiuchisan, I., Balan, D. G., Geman, O., Chiuchisan, I., & Gordin, I. (2017, June). A security approach for health care information systems. In 2017 Ehealth and bioengineering conference (EHB) (pp. 721-724). IEEE.

[12] Sonya, A., & Kavitha, G. (2021). Advanced Cryptography & Block Chain Based Cloud Environment for Secured E-Health Record. [10] Lee, Y. L., Lee, H. A., Hsu, C. Y., Kung, H. H., & Chiu, H. W. (2022). SEMRES-A triple security protected blockchain based medical record exchange structure. Computer Methods and Programs in Biomedicine, 215, 106595. [11] Abhishek, B., Panjanathan, R., Sarobin, V. R., Raja, B. E., & Narendra, M. (2022). Data security in e-health monitoring system. Materials Today: Proceedings. [12] Sharmin, S., Sarker, I. H., Shamim Kaiser, M., & Arefin, M. S. (2022). InterPlanetary File System-Based Decentralized and Secured Electronic

[13] Health Record System Using Lightweight Algorithm. In Proceedings of the International Conference on Big Data, IoT, and Machine Learning (pp. 691702). Springer, Singapore. [13] Hussien, H. M., Yasin, S. M., Udzir, N. I., Ninggal, M. I. H., & Salman, S. (2021). Blockchain technology in the healthcare industry: Trends and opportunities. Journal of Industrial Information Integration, 22, 100217. [14] Gabriel, S. J., & Sengottuvelan, P. (2021, October). An Enhanced Blockchain Technology with AES Encryption Security System for

[14] Healthcare System. In 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC) (pp. 400-405). IEEE.

[15] Boumezbeur, I., & Zarour, K. (2022). Privacy-Preserving and Access Control for Sharing Electronic Health Record using Blockchain Technology. Acta Informatica Pragensia, 11(1), 105-122.

[16] Mohammad, M. N., Kumari, C. U., Murthy, A. S. D., Jagan, B. O. L., & Saikumar, K. (2021). Implementation of online and offline product selection system using FCNN deep learning: Product analysis. Materials Today: Proceedings, 45, 2171-2178.

[17] Padmini, G. R., Rajesh, O., Raghu, K., Sree, N. M., & Apurva, C. (2021, March). Design and Analysis of 8-bit ripple Carry Adder using nine Transistor Full Adder. In 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 19821987). IEEE..

[18] Saikumar, K. (2020). RajeshV. Coronary blockage of artery for Heart diagnosis with DT Artificial Intelligence Algorithm. Int J Res Pharma Sci, 11(1), 471-479.

[19] Saikumar, K., Rajesh, V. (2020). A novel implementation heart diagnosis system based on random forest machine learning technique International Journal of Pharmaceutical Research 12, pp. 3904-3916.

[20] Raju K., Chinna Rao B., Saikumar K., Lakshman Pratap N. (2022) An Optimal Hybrid Solution to Local and Global Facial Recognition Through Machine Learning. In: Kumar P., Obaid A.J., Cengiz K., Khanna A., Balas V.E. (eds) A Fusion of Artificial Intelligence and Internet of Things for

[21] Emerging Cyber Systems. Intelligent Systems Reference Library, vol 210. Springer, Cham. https://doi.org/10.1007/978-3-030-76653-5_11

[22] Sankara Babu B., Nalajala S., Sarada K., Muniraju Naidu V., Yamsani N., Saikumar K. (2022) Machine Learning Based Online Handwritten Telugu Letters Recognition for Different Domains. In: Kumar P., Obaid A.J., Cengiz K., Khanna A., Balas V.E. (eds) A Fusion of Artificial Intelligence and

[23] Internet of Things for Emerging Cyber Systems. Intelligent Systems

[24] Reference Library, vol 210. Springer, Cham. https://doi.org/10.1007/978-3030-76653-5_12

[25] Kiran Kumar M., Kranthi Kumar S., Kalpana E., Srikanth D., Saikumar K. (2022) A Novel Implementation of Linux Based Android Platform for Client and Server. In: Kumar P., Obaid A.J., Cengiz K., Khanna A., Balas V.E. (eds) A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems. Intelligent Systems Reference Library, vol 210. Springer, Cham. https://doi.org/10.1007/978-3-030-76653-5_8

[26] Saikumar, K., Rajesh, V., Babu, B.S. (2022). Heart disease detection based on feature fusion technique with augmented classification using deep learning technology. Traitement du Signal, Vol. 39, No. 1, pp. 31-42.

[27] https://doi.org/10.18280/ts.390104

[28] Shravani, C., Krishna, G. R., Bollam, H. L., Vatambeti, R., & Saikumar, K. (2022, January). A Novel Approach for Implementing Conventional LBIST by High Execution Microprocessors. In 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 804-809). IEEE.

[29] Nagendram, S., Nag, M. S. R. K., Ahammad, S. H., Satish, K., & Saikumar, K. (2022, January). Analysis For The System Recommended Books That Are Fetched From The Available Dataset. In 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 1801-1804). IEEE.

[30] Jothsna, V., Patel, I., Raghu, K., Jahnavi, P., Reddy, K. N., & Saikumar, K. (2021, March). A Fuzzy Expert System for The Drowsiness Detection from Blink Characteristics. In 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 19761981). IEEE.