International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Improved Cyber Security in Healthcare Using an Advanced encrypted system algorithm and Blockchain Technology

Rashmi[1], Dr. S. Gunasundari[2], Swetha[3], Vidhyasree[4], Sagar[5], Kumaran[6]

Submitted: 03/02/2024 **Revised**: 11/03/2024 **Accepted**: 17/03/2024

Abstract: Protecting patients' private health information and storage is of the utmost importance in the ever-changing world of healthcare. Data security and efficiency have always been pressing issues, and an immediate need for improved cybersecurity in the healthcare industry's transition to digital records requirement by integrating compression, encryption, and storage methods. Solutions are emerging from the convergence of cutting-edge technology such as blockchain, and compression algorithms, with cloud storage. Data gathering, and pre-processing using KNN, an advanced encrypted System algorithm to encrypt the data which is in text, document, and image into hexadecimal numbers and compresses the large medical data size into small that is compressing Gb to kb then using the Blockchain technology of Hash SHA-256 algorithm data will be stored securely in the cloud. Platforms in the cloud, such as MONGO DB on AWS, securely store encrypted numerical data, guaranteeing its security and integrity only doctors or authorized workers will access and recover original information, this strategy has a responsibility to ensure accuracy, protect data confidentiality, and efficiency of the management of healthcare data

Keywords: Cyber Security, KNN, Blockchain, Encryption, Decryption, AWS, Advance Encrypted System, Hash SHA-256.

1. Introduction

Cybersecurity risks include breaches of data, and ransomware attacks, including unauthorized access to patient information due to this increasing connection. Not only may these breaches compromise patients' privacy, but they can also damage their faith in the medical system and put their safety at risk. Cybersecurity pertains to the technological measures that you must take to safeguard your networks and systems. Technological developments in the digital era are driving a sea change in the healthcare business, with the potential to increase operational efficiency, improve medical results, and redefine patient care. Digital health technology such as wearable devices, medical imaging systems, and electronic health records, or EHRs, are generating massive quantities of data and are therefore pivotal to this change. The digitalization of healthcare brings new possibilities and new problems, the most pressing of which are issues with the privacy and security of patient's health records.

[1]*PG Scholar, Velammal Engineering College, Chennai-600066, rashmi2kvec@gmail.com*
[2]*Associate Professor, Velammal Engineering College, Chennai-600066, gunasundari@velammal.edu.in*
[3] *Assistant Professor, Vel Tech High Tech Dr.Rangarajan Dr.Sakuntala Engineering College, Chennai-600062 Swetha.r@velhightech.com*
[4]*Assitant Professor, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai-600062 Vidhyasree.v@velhightech.com*
[5]*UG Scholar, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai-600062 sagartharun04@gmail.com*
[6]*UG Scholar, Velammal Engineering College, Chennai-600066, mrkumarancse@gmail.com*

Cybersecurity is primarily concerned with safeguarding a system than data protection, which focuses on information kept within a system. One potential method for improving healthcare communication and storage efficiency is data compression and keeping it secure. Medical data may be compressed using techniques that reduce its size without sacrificing its integrity. This allows for quicker transmission of data across storage systems and computer networks. However, there are security issues with sending private health information over unsecured networks, thus encryption methods must be used to protect patient privacy. Cloud computing's meteoric rise has also altered how hospitals and other medical facilities keep and make available patient records. Scalable and affordable options for storing and analysing massive volumes of healthcare data are provided by large-scale computing centres like MongoDB on AWS. However, there are further security concerns with moving sensitive medical data to the cloud since data kept on distant servers might be susceptible to data breaches and illegal access. Healthcare companies are actively seeking new ways to address these difficulties and ensure the security of medical data while making the most of digital technologies. The distributed ledger technology (blockchain) that underpins digital currencies like Bitcoin has recently attracted attention as a potential solution for protecting sensitive data in the healthcare industry and beyond.

Blockchain provides an immutable, transparent platform for the safe management of medical information by decentralized data storage and using cryptographic methods to guarantee data integrity. The use of machine

learning systems has also shown promising results when used in medical data analysis for pattern recognition, outcome prediction, and diagnostic precision. People are wary of disclosing personal health information to third-party companies since training these algorithms takes massive volumes of data. Machine learning models may be trained on decentralized data sources using secure multiparty systems computation (SMC) along with federated learning approaches, which do not compromise patient privacy, With the integration of enlargement, encryption, and storage approaches, our suggested system seeks to tackle the dual difficulties of healthcare data security and efficiency. Our technology uses powerful encryption techniques to safeguard private healthcare information from unwanted access, building upon current technologies like distributed code reuse (DSC) and stream encryption. Expedite data transfer while protecting patient privacy by integrating compression with encryption. Our solution is much more secure and scalable now that the blockchain system and cloud computing are integrated. To make sure that no one can access or steal sensitive medical information images, text, and documents are converted to encrypted numerical forms and stored safely in the cloud in MONGDB AWS. The diagram provided in Figure 1 below depicts the entire implementation process.

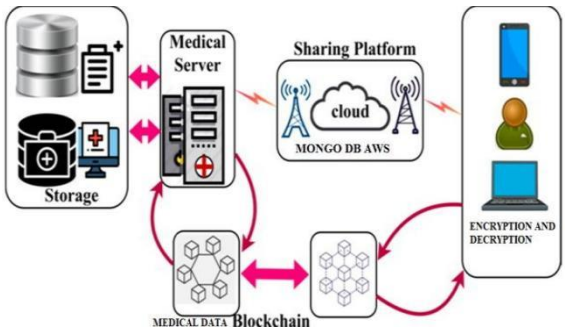

Fig. 1. Overview of the Implementation Process

2. Literature Survey

A representation digital twin and of the physical world that exists in the digital realm. Cybersecurity professionals may benefit greatly from DT as it allows them to model and test cyberattacks that would be impossible to conduct in actual time in a physical setting, and it also allows them to foresee dangers without accessing the physical world. Through the creation of a virtual representation of those targeted healthcare systems, DT aids in the identification of security vulnerabilities, the execution of attack simulations, and possible security breaches.

A proposed automated conceptual framework in the healthcare sector leverages the Internet of Things (IoT) to enhance cybersecurity [1]. This framework lays the foundation for a system capable of identifying vulnerabilities and threats in healthcare applications utilizing the IoT, providing an adaptable security solution. The major causes of healthcare data breaches were determined by this research [2]. The results of this study will undoubtedly become a benchmark for future security professionals to utilize, potentially contributing to our understanding of data breaches. The veracity of the dataset investigated is a prerequisite for all the outcomes.

Healthcare workers' demographic information, and stress levels, including cybersecurity procedures were gathered using an online study [3]. The Perceived Stress Scale, was used to measure the stress levels of the participants, and the Hospital Staff's Dangerous Cyber Practices Scale was used to evaluate the cybersecurity practices of the hospital staff. Vigilant aware, prepared, and responding quickly are the only strategies to lessen security risks and threats [4], Doable with a long-term dedication to the cause and will yield significant rewards for a robust healthcare system.

The medical field has reaped tremendous benefits from the expansion of the Internet of Things [5]. This article looks at the security problems with smart health devices and suggests some basic fixes. Protecting the IT infrastructure from threats involves more than just safeguarding hardware and software [6]. This necessity arises from the growing use of technologies like Artificial Intelligence and mobile smart devices in medical practices.

The increasing utilization of IT solutions within the healthcare industry is resulting in a gradual rise in the frequency of cybersecurity incidents [7]. Operational challenges arise from applying this massive corpus of information, and operators' resilience to cyberattacks is still lacking. The majority of healthcare organizations understand the significance of cybersecurity, as 96% of participants confirmed cybersecurity as a top priority for their organizations [8]. This research paper utilizes the 7-S Model strategy as a framework for developing strategies for healthcare organizations in the post-COVID-19 era. The use of tablet PCs by healthcare professionals to read and change patient records is growing in frequency due to the acceptance of healthcare data in the industry [9]. This paper analyses the process of leveraging the dynamic temporal warping (DTW) method of string matching in conjunction with online signature and fingerprint verification to provide reliable user authentication. Protecting sensitive data is essential since, in many nations, the healthcare system is regarded as an essential infrastructure [10]. Healthcare providers must be ready to defend against potential assaults and cyber threats. This essay describes the main cybersecurity risks with an emphasis on the healthcare industry.

Both industry and academics have recently been more interested in the metaverse. With its enormous potential and cutting-edge technology, it could completely transform every industry of healthcare [11]. Key elements of the metaverse that will be included in future healthcare systems are Avatar, Blockchain, and Extended Reality (XR). Healthcare software and cutting-edge medical equipment are essential to patient care, yet hackers frequently target them [12]. Numerous endpoints, which are the potential weak points in the system and potential entry points for unauthorized access to the medical data management network stem from the locations within the healthcare industry where data is retrieved.

The Industrial Internet of Healthcare Things (IIoHT) represents a novel healthcare system that allows various medical applications to function on hospital servers, facilitating the delivery of remote medical services [13]. This investigation presents a cyber- physical system (CPS) equipped with several heuristics, which proves to be economically efficient in managing the scheduling of blockchain tasks (CBTS). Distributed storage methods and transaction storage mechanisms are still present [14]. According to the experiments, blockchain systems that use our CI store process half as many transactions as Bloom filters and one time as many as Merkle trees.

In multimedia applications, picture encryption techniques are essential for guaranteeing the confidentiality and legitimacy of digital images used in healthcare [15]. This has brought attention to the problem that medical photographs are frequently created and distributed online, requiring safeguards against unauthorized usage. The intention behind incorporating positive DC prediction error modulo encryption is to prevent the occurrence of overflow processing, which in turn results in extended encryption durations and reduced versatility [26]. The key role of ending ACG-URSV, which encompasses zero coefficients succeeding the final non- zero AC coefficient position (PLZ), is to adjust PLZ.

The diverse range of methods, technologies, and regulations in place for protecting medical data in digital healthcare face numerous challenges. To bolster data security, privacy, and resilience in the digital era, healthcare entities can adopt a multi- layered cybersecurity approach, incorporate emerging technologies like blockchain and artificial intelligence, and promote collaboration among stakeholders. The distributed source coding method involves encrypting images in RDH. This process includes using a stream cipher to encrypt the original image or media. The data-hider then compresses specific bits from the encrypted image to create hidden data. The sender encrypts the original image directly, while the data-hider inserts extra bits by altering some of the encrypted data. During the decryption of the marked encrypted image, data extraction, and image recovery occur by analyzing the local standard deviation. Enhancing image security involves encrypting both the data and the image where the data is concealed. For data retrieval, the receiver must possess decryption keys for the data, retrieval keys for extracting data from the image, and decryption keys for the image.

3. Proposed System

Using a combination of data compression and encryption, the suggested methodology systematically improves healthcare cybersecurity. Protecting the security, efficacy, and accuracy of the management of healthcare data is the responsibility of each level of the approach. the proposed system preprocesses the collected medical data with the KNN algorithm for clustering, and integrates the ASE algorithm for encryption to protect patient private data into a numerical format to hide the original medical data, so data compression is done meanwhile, data will be stored in the cloud securely by Hash algorithm in blockchain technology in Mongo database on AWS for access controls this can be seen in the diagram figure 2 given below.

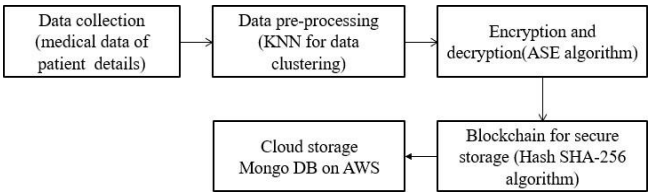

Fig. 2. Proposed System

3.1. Data Collection

This phase entails collecting health information from a variety of sources, including wearable devices, diagnostic imaging technologies, medical equipment, and electronic health records (EHRs). Patients' data, such as names, genders, test outcomes, diagnosed illnesses, prescribed therapies, and medical records, is collected and compiled into a dataset. Adherence to privacy regulations, like the Health Insurance Portability and Accountability Act (HIPAA), is crucial to safeguarding the confidentiality and security of patient information. Streaming in real-time, processing data in batches, or integrating directly with current healthcare systems are all possible ways to get data normal records have been pre-processed.

3.2. Preprocessing

The collected data is cleaned, normalized, and transformed into a standard format for future analysis during pre-processing before encryption and storage. Data cleaning, dimensionality reduction, feature scaling,

and outlier identification are all examples of pre-processing methods as shown in the below figure

3. Now is the time to make sure that data is consistent and of high quality so that your analysis can be more accurate and reliable in grouping the data under various categories of diagnosed treatment.

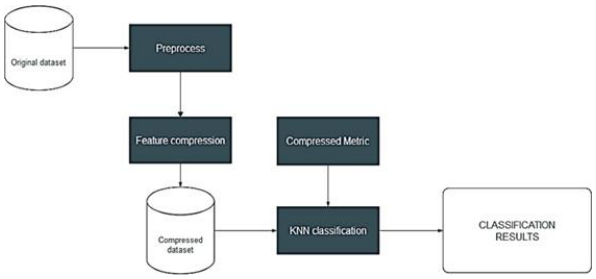

Fig .3. Data Preprocessing

3.3. KNN Algorithm

The most frequently used method in the K-neighbours classification. The ideal number for K depends heavily on the data, a bigger value reduces the impacts of noise but lowers the boundaries of the classification. Uniform weights are used in the basic nearest neighbors classification, meaning that a query point's value is determined by the nearest neighbors casting a simple majority vote. The K-NN technique assigns the new case to the most similar category among the existing ones in the dataset. This involves classifying data points using the k-NN algorithm, which utilizes similarity and retains all available data. Essentially, the K-NN algorithm efficiently categorizes the dataset obtained from data pre-processing.

KNN pseudocode:

- Selecting the value of K
- Determining distances between points in thetraining set,
- Determine the K closest neighbors using the computed distances.
- Give the new data point the majority classlabel.
- Analyzing the algorithm's accuracy throughtesting.

By utilizing the K-NN algorithm on around 900 patient datasets containing patient numbers, names, and treatment categories shown in Table 1, a clustering process is initiated. This clustering enables the secure encryption and storage of medical data in the cloud by grouping patient datasets efficiently. During the training phase, the KNN algorithm simply stores the dataset and categorizes new medical data based on its similarity to existing data.

212302	1877191	00 Zuniga	Physician Assistant	1
218789	1877036	70 Zhang	Nurse Practitioner	0.9
212006	1877167	26 Yoder	Nurse Practitioner	1
212780	1877208	94 Yates	Nurse Practitioner	1
214964	1877144	66 Willi	Nurse Practitioner	0.57
218309	1877034	71 Willi	Nurse Practitioner	0.28
212304	1877207	66 Wiggi	Dental Hygie - Clinical	0.09
216277	1877142	08 Wells	Physician Assistant	0.6
213945	1877055	66 Webst	Nurse Practitioner	1
216570	1877111	52 Watts	Physician Assistant	0.26
216635	1877192	56 Waiss	Nurse Practitioner	0.9
216020	1877105	28 Volce	Nurse Practitioner	1
218351	1877135	28 Velez	Nurse Practitioner	1
212100	1877192	00 Vega	Nurse Practitioner	1
216815	1877152	34 Vasques	Physician Assistant	0.25
212545	1877197	62 Vance	Physician Assistant	1
216124	1877018	18 Valencia	Nurse Practitioner	0.6
213833	1877155	64 Tyler	Nurse Practitioner	1
216070	1877155	06 Turner	Physician Assistant	0.9
216725	1877051	72 Trevino	Nurse Practitioner	0.9
218870	1877060	52 Strong	Nurse Practitioner	0.9
214561	1877225	90 Sorc	Physician Assistant	1
216500	1877048	16 Sodo	Nurse Practitioner	1
217513	1877141	98 Snyder	Physician Assistant	0.9
216881	1877073	56 Simpson	Physician Assistant	0.9
216596	1877236	42 Sharp	Nurse Practitioner	0.75
217240	1877152	22 Sellers	Physician Assistant	0.17
218996	1877147	40 Schmidt	Nurse Practitioner	1
217305	1877067	76 Saunders	Physician Assistant	0.4
218974	1877168	90 Santiago	Physician Assistant	1
214977	1877071	76 Sanchez	Physician Assistant	1
218699	1877214	91 Salas	Registered Nurse	1
218844	1877167	16 Ruy	Physician Assistant	1
218918	1877157	20 Roth	Physician Assistant	0.13
216912	1877156	14 Rivera	Physician Assistant	1
217290	1877151	72 Ritter	Nurse Practitioner	0.75
216879	1876899	46 Rich	Physician Assistant	0.14
217205	1877211	76 Rice	Physician Assistant	1
215196	1877156	32 Reyes	Physician Assistant	0.9
212224	1877126	26 Reed	Nurse Practitioner	1
216295	1877174	18 Raymond	Nurse Practitioner	0.9
217202	1877156	18 Ramussen	Nurse Practitioner	0.5
216910	1877186	34 Mandel	Nurse Practitioner	1
214234	1877157	62 Prince	Nurse Practitioner	1
218316	1877186	41 Powell	Nurse Practitioner	1
216208	1877256	68 Poole	Nurse Practitioner	0.5
218295	1877053	21 Ponce	Physician Assistant	1

Table 1. Clustered Dataset of Patients

3.4. Advanced Encryption System Algorithm

The preprocessed data is encrypted using advanced encryption algorithms before storage. Here, most of the government and commercial sector IT security applications currently use the Advanced Encryption System (AES) as their encryption standard. AES 256-bit encryption is the most robust encryption standard. AES encryption methods are used to safeguard the pre-processed data from any potential illegal access while it is being sent or stored. After obtaining a dataset containing both text and images, by the AES algorithm, the encryption procedure to convert the string to hexadecimal value will be done as shown in the block diagram given below in Figure 4.

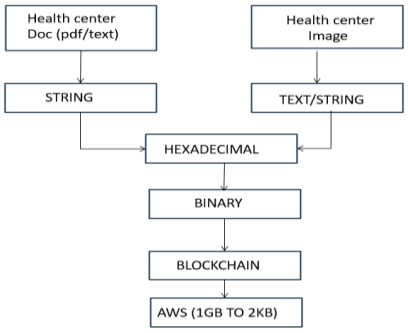

Fig.4. Converting string to encrypted numerical value

The proposed system employs advanced encryption system techniques, including symmetric-key encryption, asymmetric encryption, and homomorphic encryption, to protect medical data at rest, in transit, and use. By encrypting sensitive information using robust cryptographic algorithms and securely managing encryption keys, the proposed system ensures the confidentiality and integrity of patient records, diagnostic images, and other healthcare data. The module employs cutting-edge encryption methods to shield data from unauthorized access both during transmission and storage. The method uses database scan techniques and the Blockchain to encrypt and compress medical data before converting it to numerical form. Encrypted numerical data is safely stored on cloud platforms like MONGO DB. The original data may be decrypted and accessed by authorized users whenever necessary since the decryption keys are safely handled and preserved. When authorized users require access, decryption algorithms are applied to retrieve the original data securely.

3.5. Blockchain technology

The blockchain achieves its promises of decentralization and safe, transparent transactions. They keep the blockchain's general integrity intact, verify transactions, and enable peer-to-peer interactions. Since cryptography is used to link these lists, it is the most basic prerequisite for building a blockchain. Blockchain is a continuously growing collection of records achieved by adding new blocks over time. By utilizing a cipher, a hash table transforms the text into a hash value of a specific length. Decrypting the ciphertext to retrieve the original text is a challenging process. Through mathematical cryptographic methods, data is both encoded and decoded, making it incomprehensible to unauthorized individuals lacking the appropriate decryption key. This heightened security measure significantly reduces the risk of unauthorized access to and modification of data stored on the blockchain.

3.5.1 Hash SHA-256 Algorithm

Blockchain employs a cryptographic hash function to connect the blocks sequentially and safeguard the information within each block. Each block within the chain contains a hash of the previous block along with its hash. The Secure Hash Algorithm, known as SHA-256, creates a 256-bit summary of a data message. This hashing method is widely recognized and utilized by numerous digital currencies. Through this process, the encoded hexadecimal data from the previous step is stored within the hash table as shown in Figure 5.

Steps to process a message using the SHA-256 Algorithm:

1. **the message size to be a multiple of 512:** adding the initial message with a few extras. The overall length is therefore precisely 64 bits shorter than a multiple of 512. The message M has a length of L. It indicates that L+P+64 equals n*512, where L is the message's length and P is its padding in bits.

2. **Add length bits (Padding Length)**: calculate the 64 bits, L (the original length of the message) mod 2^{32}. So, to get the entire message block, L+P+ [L mod 2^{32}] = n*512.

3. **Initialize Chaining Variable**: The message is divided into n 512-bit blocks. For example, M1, M2, M3...Mn.

4. **Proceed with each block:** The message is divided into nblocks, each containing 512 bits. There are 16 sub- blocks of 32 bits apiece within each 512-bit block.

64 rounds of operations are conducted. Additionally, the output produced will be used as input for the next set of tasks.

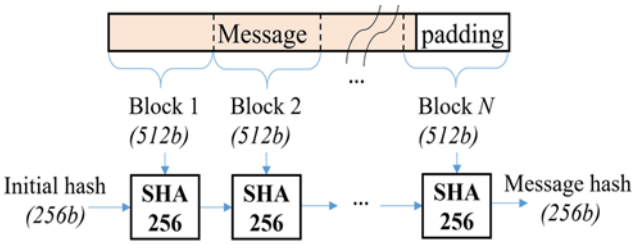

Fig.5. SHA-256 hash value

3.6. Cloud Storage and Access Control

With the use of access control techniques, encrypted healthcare data may be regulated and restricted to users according to their responsibilities and permissions. Common methods for enforcing access regulations include role-based and attribute- based controls as well as multi-factor authentication. One of the most versatile features of NoSQL databases is MongoDB. It enables you to work with and save several data kinds in a single document. Moreover, MongoDB can hold significantly more data than relational databases. These core characteristics of MongoDB are a result of the JSON document storage format that the database system uses.

Using AWS Identity and Access Management (IAM), account roles, and two-step verification, you can manage who has access to your AWS account. Account roles and two-step verification go without saying, but Identity and Access Management (IAM) is a feature-rich platform that lets you manage access, check account activity, and create alerts. Robust encryption and authentication Through authentication, the identity of a person requesting access to a system is confirmed. Information is protected using encryption by being encoded in a way that renders it unintelligible to those lacking the decryption key.

4. Implementation and Result

Outcomes of the suggested approach to improving healthcare cybersecurity utilizing combined information compression and encryption. The first step in protecting sensitive medical data is using strong encryption methods at every stage of its lifetime, from information obtained from the healthcare sector to storage to transfer. The dataset includes test results, diagnosis of the illness, conducted treatments, personal information, and physician recommendations. The gathered data was categorized using the KNN algorithm for subsequent conversion into a string that contains both text and images The pre-processed data during transmission or storage to prevent any possible unauthorized access. By the KNN algorithm, the clustering is done by data gathered from pre-processing information of patient's personal information, diagnosed problems, treatment done, and report of the patient. Transform the dataset which includes both text and images into a string. Next, will convert the string to hexadecimal, which is a numerical format, Figure 6. below illustrates the patient's data input, which includes text and image access by the doctor and authenticated workers in the healthcare center, using the advanced system Encryption (ASE) algorithm for encryption and decryption.

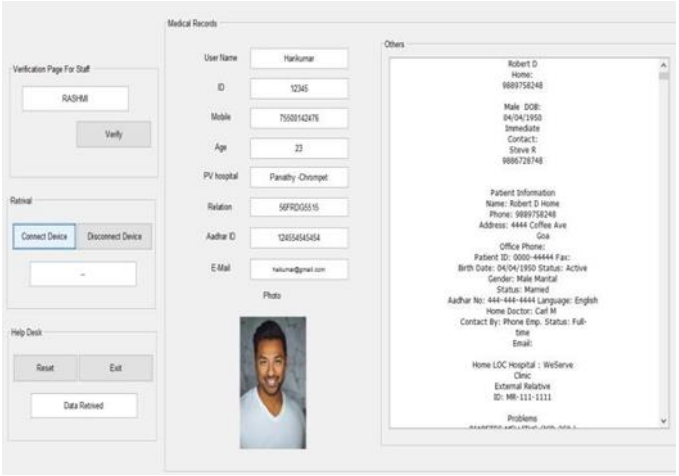

Fig. 6. Input to Convert Patient Data

Following input, the string is encrypted and transformed to a hexadecimal value. The resultant numerical value, which is the original information, will then be encrypted and stored secretly using blockchain technology using a hash algorithm. Supply chain networks across all industries can utilize Amazon Managed Blockchain for tracking changes on a unified ledger, providing them with full visibility of data and a reliable source of truth. To query the blockchain or add new blocks to the chain, each block that is generated must be kept in one central location. The ledger of blockchain may be stored in MongoDB Atlas, the database-as- a-service cloud service from Mongo DB. To ensure that written files and data are encrypted while being stored, encryption at rest is a database-level security layer. AES-256 at-rest encryption has been introduced by MongoDB Enterprise Advanced (EA) in Wired, the database storage engine below Figure 7. displays the conversion of hexadecimal value by encryption and stores in MongoDB AWS.

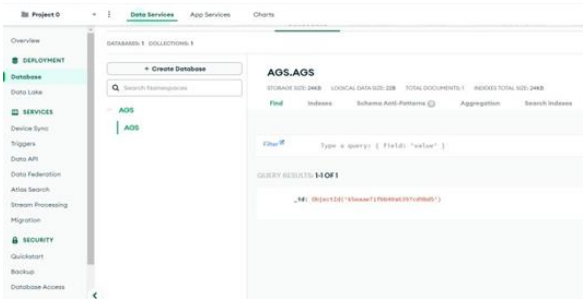

Fig.7. Output value in Hexadecimal stored in cloud

Mongo DB

Secure transmission methods protect healthcare data from prying eyes by encrypting data packets and authenticating connection endpoints. This prevents eavesdropping, manipulation, and man- in-the-middle attacks. Hexadecimal sequences produced by mathematical methods are known as hash values. Data that is added to the blockchain is first hashed that is, transformed text into a string then encryption algorithm using cryptographic methods, and then saved on the

blockchain in Mongo DB. The efficacy and safety of the suggested methods depend on constant monitoring and updates. Finally, the research shows that the suggested approach improves healthcare cybersecurity by combining data compression for keeping data securely by hiding the original medical data using the ASE algorithm of encryption methods with the integrated blockchain technology of Hash SHA-256 algorithm for secure cloud storage in Mongo DB on AWS. The original information will be accessed and recovered by a doctor or other authorized employees. This strategy is responsible for guaranteeing accuracy, safeguarding data confidentiality, and optimizing the effectiveness of healthcare data management.

5. Conclusion and Future work

Safeguarding confidential patient health data and its preservation is crucial in the rapidly evolving healthcare industry. As the healthcare sector moves towards requiring digital records, data security and efficiency have always been critical concerns. Improving cybersecurity through the integration of compression, encryption, and storage techniques is urgently needed. Innovative technologies like compression algorithms and blockchain are coming together with cloud storage to provide solutions. The data collection, KNN pre-processing, encryption /decryption technique, and prediction are the four main components of our proposed system. By encryption and compressing methods converting medical data into numerical form using the Advance System Encryption algorithm, the solution uses database scan methods to store data using the blockchain technology using the Hash SHA-256 algorithm. Cloud-based platforms, like MONGO DB, ensure the security of encrypted numerical data by securely storing it. Finally, by combining data compression with encryption approaches the suggested methodology offers a thorough framework to improve security in healthcare cybersecurity. In addition, our study's findings show that healthcare data management might benefit from using data encrypting and compression methods, which could lead to increased efficiency, better security, and compliance with regulations. Develop trust, resilience, and security in the healthcare digital ecosystem by prioritizing cybercrime and investing in comprehensive data protection measures. This will ensure the safety and security of patient data for centuries.

This medical data can use statistical modeling or machine learning approaches after encryption to identify trends, patterns, or outliers of predictive analytics, such as disease diagnosis, treatment optimization, patient outcome prediction, and community health management, which are routine prediction issues in healthcare for future enhancement

References

[1] S. Pirbhulal, H. Abie and A. Shukla, "Towards a Novel Framework for Reinforcing Cybersecurity using Digital Twins in IoT-based Healthcare Applications," 2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring), Helsinki, Finland, 2022, pp. 1-5, Doi: 10.1109/VTC2022-Spring54318.2022.9860581.

[2] M. George-Bogdan and G. Meşniţă, "Healthcare under siege: the need to improve cybersecurity in the near future," 2022 E-Health and Bioengineering Conference (EHB), Iasi, Romania, 2022, pp. 1-4, Doi: 10.1109/EHB55594.2022.9991541.

[3] M. P. Carello, A. Marchetti-Spaccamela, L. Querzoni and M. Angelini, "SoK: Cybersecurity Regulations, Standards and Guidelines for the Healthcare Sector *," 2023 IEEE International Conference on Intelligence and Security Informatics (ISI), Charlotte, NC, USA, 2023, pp. 1-6, Doi: 10.1109/ISI58743.2023.10297246.

[4] A. Alghamdi, "Cybersecurity threats to Healthcare Sectors during Covid-19," 2022 2nd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 2022, pp. 87-92, doi: 10.1109/ICCIT52419.2022.9711659.

[5] A. M. Mohamad Al-Aboosi, S. N. Huda Sheikh Abdullah, M. Z. Murah and G. S. AL Dharani, "Cybersecurity Trends in Health Information Systems," 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 2022, pp. 01-04, Doi: 10.1109/ICCR56254.2022.9995952.

[6] V. M. Nguyen and A. Y. Nur, "Major Cybersecurity Threats in Healthcare During Covid-19 Pandemic," 2023 International Symposium on Networks, Computers, and Communications (ISNCC), Doha, Qatar, 2023, pp. 1-8, Doi: 10.1109/ISNCC58260.2023.10323723.

[7] R. Prakash, G. R. Nayar and T. Thomas, "Security Risk Assessment of Metaverse Based Healthcare Systems Based on Common Vulnerabilities and Exposures (CVE)," 2023 IEEE International Conference on Recent Advances in Systems Science and Engineering (RASSE), Kerala, India, 2023, pp. 1-10, Doi: 10.1109/RASSE60029.2023.10363519.

[8] Mohan, A., Prabha, G. and V., A. 2023. Multi Sensor System and Automatic Shutters for Bridge-An Approach. International Journal of Intelligent Systems and Applications in Engineering. 11, 4s

(Feb. 2023), 278–281.

[9] Prabha , G. , Mohan, A. , Kumar, R.D. and Velrajkumar, G. 2023. Computational Analogies of Polyvinyl Alcohol Fibres Processed Intellgent Systems with Ferrocement Slabs. International Journal of Intelligent Systems and Applications in Engineering. 11, 4s (Feb. 2023), 313–321.

[10] Study On Structural Behaviour Of Ductile High-Performance Concrete Under Impact And Penetration Loads, Lavanayaprabha, S. Mohan, A. Velrajkumar, G., Mohammedharoonzubair, A. Journal of Environmental Protection and Ecology., 2022, 23(6), pp. 2380–2388.`

[11] Vidhya Lakshmi Sivakumar, A.S. Vickram, Ragi Krishnan, Titus Richard, "AI-Enhanced Decision Support Systems for Optimizing Hazardous Waste Handling in Civil Engineering," SSRG International of civil Engineering. Vol 10, 2023.

[12] Mohan, A., Dinesh Kumar, R. and J., S. 2023. Simulation for Modified Bitumen Incorporated with Crumb Rubber Waste for Flexible Pavement. International Journal of Intelligent Systems and Applications in Engineering. 11, 4s (Feb. 2023), 56– 60.

[13] R.Gopalakrishnan, Mohan, “Characterisation on Toughness Property of Self-Compacting Fibre Reinforced Concrete”, Journal of Environmental Protection and Ecology 21, No 6, 2153–2163 (2020)

[14] Mohan, A., Dinesh Kumar, R. and J., S. 2023. Simulation for Modified Bitumen Incorporated with Crumb Rubber Waste for Flexible Pavement. International Journal of Intelligent Systems and Applications in Engineering. 11, 4s (Feb. 2023), 56–60.

[15] D., G. ., Ramar, A. ., Karpagam, S. ., J., S. ., S., R. ., & P., S. . (2024). Sign Language Recognition Using Convolutional Neural Network. International Journal of Intelligent Systems and Applications in Engineering, 12(17s), 329–337.

[16] P. Soni, J. Pradhan, A. K. Pal, and S. H. Islam, "Cybersecurity Attack-Resilience Authentication Mechanism for Intelligent Healthcare System," in *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 830-840, Jan. 2023, Doi: 10.1109/TII.2022.3179429.

[17] Lakhan, M. A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari and N. Kumar, "Blockchain-Enabled Cybersecurity Efficient IIOHT Cyber-Physical System for Medical Applications," in IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, pp. 2466-2479, 1 Sept.-Oct. 2023, doi: 10.1109/TNSE.2022.3213651.

[18] X. Feng, J. Ma, H. Wang, S. Wen, Y. Xiang and Y. Miao, "Space-Efficient Storage Structure of Blockchain Transactions Supporting Secure Verification," in IEEE Transactions on Cloud Computing, vol. 11, no. 3, pp. 2631-2645, 1 July-Sept. 2023, Doi: 10.1109/TCC.2022.3220664.