SAFEGUARDING HEALTHCARE DATA PRIVACY IN THE CLOUD USING MODIFIED FUZZY PARTICLE SWARM OPTIMIZATION AND TWO FISH ENCRYPTION ALGORITHM

Suresh Kumar Maddila[1], Dr. Nagalakshmi Vadlamani[2]

[1]Research Scholar, Department of Computer Science, GITAM (Deemed to be University), Visakhapatnam, Andhra Pradesh, India.

[2]Professor, Department of Computer Science, GITAM (Deemed to be University), Visakhapatnam, Andhra Pradesh, India.

DOI: https://www.doi.org/10.58257/IJPREMS35447

ABSTRACT

In the healthcare field, merging different sets of data is crucial for the future. Cloud computing offers a way to efficiently handle this diverse data. Cloud computing has made it easier for people to access services and resources, but it also means we need better security to deal with new threats. This paper proposes a novel method for securing data stored in the cloud. It uses the Two Fish encryption algorithm and the Bald Eagle Pelican Optimization algorithm (BEPO) to create keys for security. To keep medical records safe when they're sent, a new system called Blockchain based Privacy Preserving and Robust Healthcare data (BPPRH) is introduced. It goes through different steps like setting up, registering, encrypting, checking, and decoding. The Twofish along with BEPO key generation method offers strong security procedures such as conditional privacy, time taken for validation, usage of memory, and normalized variance. The system uses a hypervisor and virtual machines (VMs) to protect against different types of attacks. The proposed Modified Fuzzy Particle Swarm Optimization (MFPSO) method helps to detect threats. Another method, Edge Cloud based Collaborative Systems (ECCS), uses advanced techniques to reduce risks, achieving a high accuracy rate of 99.32%. This enhanced system improves the security of healthcare management systems, dealing with problems in traditional smart healthcare systems.

Keywords: Encryption, Key generation, Twofish algorithm, Cloud Computing, Optimization, Privacy Preserving, Healthcare Data.

1. INTRODUCTION

The healthcare sector has embraced cloud computing, utilizing its infrastructure to seamlessly gather data from diverse sources and facilitate efficient data integration. However, alongside its advantages in affordability and disaster recovery, ensuring robust security remains a critical concern in cloud computing adoption [1]. Unprotected data transmitted over networks or stored in cloud services risk manipulation or loss, potentially endangering patient lives. Moreover, the inherent vulnerability of cloud systems may expose sensitive healthcare information to malicious actors, underscoring the imperative for enhanced security measures.

To address these challenges, we propose a comprehensive style to safeguard healthcare data [2] in the cloud. Leveraging the Two fish encryption algorithm and optimization-based algorithm like Bald Eagle Pelican Optimization Algorithm for key generation, our novel Twofish along with BEPO based Key Generation method offers a multi-faceted solution. Through phases including initialization, registration, encryption, authentication, and decryption, this approach ensures robust security metrics, including usage of memory, time it is taking for validation, conditional privacy and normalized variance. In addition to encryption, our solution integrates blockchain technology to establish a secure patient information. This Blockchain enabled Privacy Preserving system for healthcare data system enhances data integrity and confidentiality during transmission and storage. Furthermore, by deploying a hypervisor and virtual machines (VMs) within the cloud infrastructure, the proposed method supports to handle several network attacks.

The use of MFPSO improves the identification of potential threats. Simultaneously, ECCS strategy reduces risks by using sophisticated methods like regularized maximum likelihood estimation and shadow model reconstruction. Our comprehensive approach not only improves the security of healthcare management systems but also addresses the common security weaknesses found in traditional healthcare models.

Cloud computing transforms how programs and data are accessed and managed by providing universal access to shared computing resources via the internet. With cloud services provided dynamically by vendors like Amazon and Google, users can access applications and files from any device, eliminating the constraints of physical storage. However, concerns regarding data security and vulnerability persist, necessitating stringent encryption and authentication measures.

In the healthcare domain, cloud computing facilitates the continual gathering and integration of diverse data sources, streamlining processes and enhancing accessibility to critical information. Yet, the storage of sensitive healthcare data in cloud environments introduces new challenges in data confidentiality and integrity. The responsibility lies with Cloud Service Providers (CSPs) to ensure secure storage and access, implementing robust security protocols to thwart breaches and unauthorized access attempts.

Despite the benefits of cloud computing, including cost efficiency and scalability, concerns persist regarding data privacy and security. Encryption techniques are increasingly employed to safeguard sensitive information, yet challenges in interoperability and resource sharing persist. These challenges underscore the need for innovative solutions that balance usability with stringent privacy protection measures.

To address these challenges, our research presents a comprehensive strategy for securing healthcare data in cloud environments. By incorporating encryption algorithms, optimization techniques, and blockchain-based privacy mechanisms, our solution aims to enhance integrity of medical data and security of the data while ensuring it remains interoperable and accessible across different healthcare systems. Through strict analysis and our assessment strategies, we demonstrate the effectiveness of our planned approach in meeting the evolving security needs of cloud-based healthcare systems.

2. LITERATURE SURVEY

The healthcare sector has increasingly relied on cloud computing for various tasks, including data storage and transmission. Several approaches have been proposed to ensure the safe transmission of healthcare information through the cloud. One such approach is the privacy preserving method using blockchain method to secure transmission of patient data while ensuring privacy.

To avoid confidential data from being leaked by server backends, Xie et al. [22] proposed an improved RFID based authentication protocol focused on safety. This protocol has been extended to integrate with the cloud environment, storing tag information on cloud servers. Meanwhile, Cao et al. [23] introduced a hybrid approach for blockchain based systems for sharing health data reports, addressing privacy and integrity of the data. This system employs consortium blockchains for privacy-sensitive data and public blockchains for non-sensitive data.

Qiu et al. [15] presented a robust method for data storage and distribution that enhances data security and privacy through a combination of partial encryption and dispersal [3]. Boumezbeur et al. [21] proposed a solution for privacy preserving for sharing and controlling the accessing mechanisms for medical data using blockchain. This platform sets user access permissions and employs the Ethereum blockchain to ensure secure record maintenance.

Rawashdeh et al. [16] futured an intrusion anomaly detection method for the layers of hypervisor to prevent DDoS attacks. Zou et al. [24] introduced SP Chain for data exchange system for medical data using which is a blockchain. It ensures privacy and efficient data retrieval. Nguyen et al. [25] developed an Electronic Health Record (EHR) sharing application using IPFS under blockchain to protect health data during cloud transfers[6].

Mehmood [12] suggested an authentication scheme to provide users of health apps with privacy and anonymity. Sahoo [26] presented a probabilistic based method using Parallel Semi Naive Bayes for clinical data processing in the cloud. Elhoseny et al. [27] presented a hybrid approach to protect medical data that includes images.

Several researchers proposed frameworks for secure data sharing and authentication in healthcare systems using blockchain and deep learning. Kumar et al. [9][10]developed a blockchain-based secure framework for IoT-enabled healthcare systems. Kumar et al. [10] also announced distributed data storage method for data sharing.

Goyal [17] established a hybrid encryption algorithm to ensure data security in cloud storage [11], while Seth et al. [14] presented a Homomorphic encryption with Blowfish algorithm for securing cloud-stored data. Sohal and Sharma utilized symmetric key encryption based on DNA cryptography for cloud security. Thabit et al. [28] proposed a key coding technique using gene based homologous, and Namasudra et al. [18] presented data security for cloud data using DNA cryptography.

Additionally, Namasudra [18] proposed an enhanced Attribute Based Encryption method. These approaches are designed to tackle various security challenges in cloud-based healthcare systems, to ensure the confidentiality and integrity of data.

3. PROPOSED METHODOLOGY

The method we propose aims to keep important health information safe when it's being stored or moved around. It begins by gathering data from doctors, healthcare workers, wearable devices, and places that hold patients' past information. Our way makes sure that everyone involved, like doctors, patients, healthcare managers, and insurance workers, can keep their privacy and have the right access to the data, all within a cloud system. To address this challenge, we introduce the 'Blockchain based Privacy Preserving and Robust Healthcare Data' method for securely transferring medical data [29].

In our literature study, it was examined all the existing blockchain based solutions for storing and sharing medical data in the cloud, identifying gaps in current research. Usually, all the medical records of hospitals are naturally stored in separate and individual databases. So, to manage all such medical data effectively, we propose a blockchain based method rereferred as BPPRH. This encrypts data stored in the cloud and grants access only to authorized users. Moreover, we model the transfer of medical data to patients via the cloud using a hypervisor and virtual machines (VM). During data transfer, potential threats such as man in the middle attacks, malwares, DoS, ransomware, and malicious users may occur, risking the theft of personal data. To mitigate these threats, we introduce a 'Modified Fuzzy Particle Swarm Optimization Algorithm' [8]. Additionally, we propose 'Edge Cloud based Collaborative Systems' to enhance security during data transfer to patients, thereby preventing such attacks.

3.1 Proposed method Blockchain based Privacy Preserving and Healthcare Data (BPPRH)

The proposed method BPPRH is extremely reliable for cloud-based healthcare data transactions. This technique involves using a public key to encrypt the data before uploading it to the cloud. To decode the data back into health records, a private key is used after receiving the encoded data. Figure 1 illustrates the cloud environment for encrypting and decrypting healthcare data. This method primarily manages the exchange of healthcare data. When patient X undergoes an examination, a record is created indicating that individual Y can able to access to X's medical report.

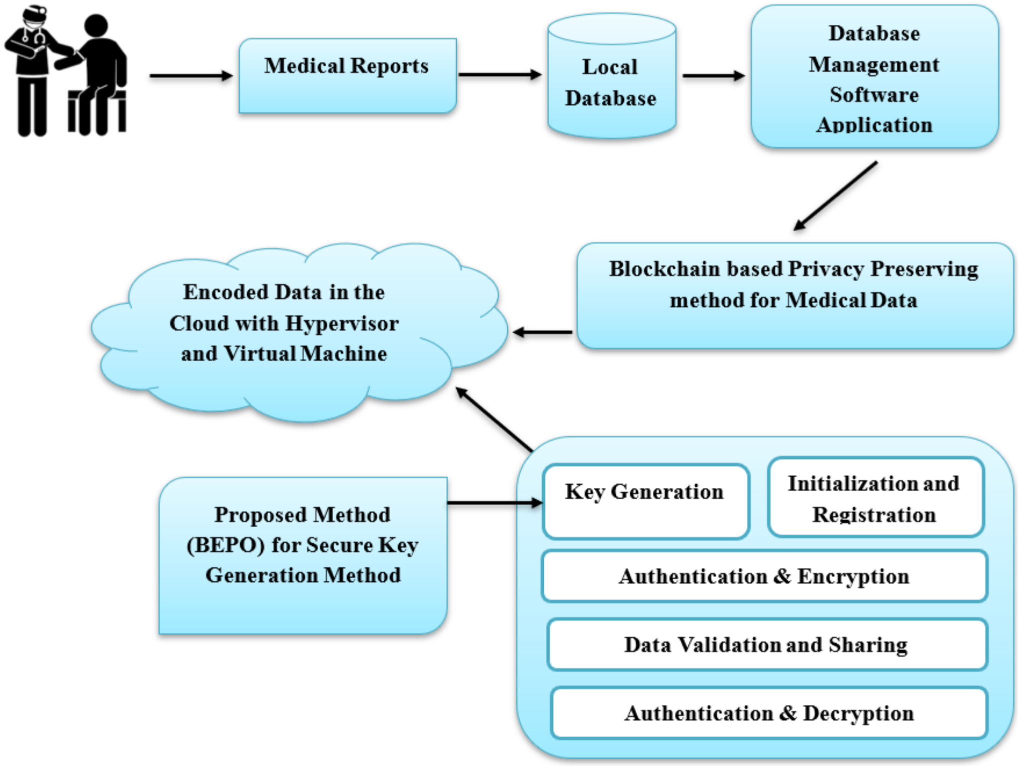
Medical Reports
Local Database
Database Management Software Application
Blockchain based Privacy Preserving method for Medical Data
Encoded Data in the Cloud with Hypervisor and Virtual Machine
Proposed Method (BEPO) for Secure Key Generation Method
Key Generation
Initialization and Registration
Authentication & Encryption
Data Validation and Sharing
Authentication & Decryption

Figure 1. Illustration of the proposed work for System Model of the Cloud

3.2 Cloud Deployment Model

Several virtual machines managed by the hypervisor enable the sharing of a cloud provider's physical computing and memory resources. These virtual machines hosted by hypervisors have access to performance data, allowing users to understand what's happening within a virtual machine without accessing its private and confidential data. In our study, a finite set of hypervisors are represented by HY = {hy_1, hy_2, ..., hy_n}, where each hypervisor hy_i in HY hosts a set of virtual machines VM = {vm_1, vm_2, ..., vm_n}. It's important to note that if the context allows, use VM instead of VM_i. Each virtual machine, VMj, within a hypervisor's VM collection is under the ownership of a client selected from the set CL = {cl_1, cl_2, ..., cl_m}.

The supervisory apparatus within HY, operating as a software intermediary, bridges the gap among VMs and hardware components of the system within cloud infrastructure.

Its function involves emulating hardware components I = {I_1, I_2, ..., I_n} and manages VM access to allow numerous virtual machines to operate concurrently on the identical cloud infrastructure. AVM is defined as a duo of O and A, where O stands for the operating system and A represents the suite of applications operating within the VM.

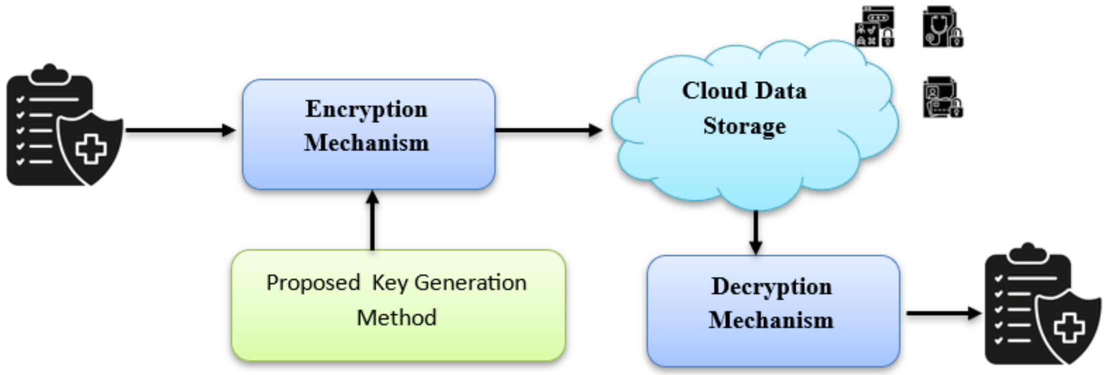

Figure 2. Illustration of secured cloud environment

In the initial stage, the hypervisor endeavors to establish trusted relationships with its guest virtual machines. It screens and examines the memory and CPU usage of all VMs. Consequently, it generates a trustworthiness measure for all VMs which are referred to initial edge cloud-based system. The hypervisor hy_0 sets the number of questions per source, allowing each source to contribute to the trust creation process. Initially, both sources receive equal numbers of requests, but modifications are made later stage. Afterwards, the hypervisor merges the results of the monitoring phase with a classification technique to create the final edge cloud based collaborative system, assigning a trustworthiness value to each virtual machine.

3.3 Key Generation Strategy

3.3.1 Initialization

Ensuring the security of data transmission starts by setting up several parameters, such as random numbers and employing public key security at the Cloud Service Provider (CSP). The random numbers are assigned values between 0 and 1. Additionally, the CSP initializes various functions including hashing, modulo operations, and Chebyshev polynomials.

3.3.2 Data owner registration step

Once the initial and crucial parameters are established at CSP to ensure secure data transfer, the next step is the registration of users and data owners with the CSP. This registration process occurs in two stages: owner registration and user registration.

The process begins with the data owner, typically a company or individual utilizing cloud services, registering with the Cloud Service Provider (CSP) to gain access to these services. During the registration time, the data owner provides personal data such credentials with the CSP. Afterwards, the CSP create an authentication message, B1, by combining the credentials received during registration, applying the modulus operation with the given random number (r). Mathematically, this is expressed as B1 = h(password || mod r), where "mod" denotes the modulus operator, "||" signifies concatenation, and "h" is a hash function. Subsequently, The CSP sends message B1 to the data owner. Then, the owner must input this message back to the CSP. If the generated message matches the owner's message, the registration is considered successful.

3.3.2 User registration step

This step is similar to the owner registration process but includes an additional authorization step. Initially, the user essentially provides his credentials, including their ID (YID), password (Ypwd), and his mobile number (YN). The owner keeps a duplicate of these credentials and sends them as Y** to the CSP. After validating the user with their credentials, the CSP generates a one-time password (OTP) and sends it back to the user. Submitting this OTP to the CSP is mandatory to complete the registration process. If the OTP does not match, it indicates an unsuccessful registration; otherwise, it is considered completed. The CSP creates the OTP by performing an XOR operation on a random number 's' and the hashed result obtained from concatenating the stored user password with the modulus value of 'b'.

3.3.3 Key generation process

After the user registers, the CSP (Cloud Service Provider) creates a private key for the user. This key is essential to uphold the integrity and confidentiality of data during communication between the user and the CSP, ensuring that unauthorized access to user credentials is prevented. The private key is generated by applying the XOR operation with the provided random number 's'. Then, it is combined with the modulus value of 'b' and the hashed values, also obtained through XOR operation, of the previously stored user credentials. Then the CSP will create private key and share it with the user.

3.3.4 Encryption with Two fish encryption algorithm

After registration with the CSP, the owner gains permission to transfer their information to the cloud. To ensure data security, the owner employs the Two fish encryption algorithm for encryption. This algorithm encrypts the data by processing the input data through Two fish encryption. The encoded data produced is denoted as X = TE(G, A). Here, X is an encrypted data, G is the input data and Two Fish encryption symbolized as TE, finally the 'A' stands for the key which produced by the proposed BEPO algorithm, which is employed for data encryption. The cloud stores the outsourced data as X* under the supervision of the CSP. The subsequent section provides a comprehensive explanation of the Two fish encryption algorithm.

The data encryption process utilizes the Twofish encryption method, employing a symmetric key block cipher for both encryption and decryption [30]. It supports both 128-bit and 256-bit blocks. Twofish is highly adaptable and ideal for networks requiring frequent key changes. It follows a Feistel structure. Half of the text block undergoes an XOR operation with the other half, which has been processed through the F-function. In each iteration, two sets of 32-bit words serve as inputs to the F-function, which are subsequently divided into four bytes. These four bytes undergo transformation through four distinct S-boxes dependent on the key. Subsequently, the resulting outputs are combined using Maximum Distance Separable (MDS) matrices before amalgamating into a single 32-bit word. The Pseudo Hadamard Transform (PHT) merges the two 32-bit words, which are then augmented by two round sub-keys and XORed with the right half of the text block. Furthermore, a 1-bit rotation is applied both before and after the XOR operation. Prior to the first round and following the last round, the text block undergoes XOR operation with additional "pre-whitening" and "post-whitening" sub-keys. Many encryption algorithms incorporate a key-setup phase wherein keys generate round sub-keys and key-dependent S-boxes. Twofish excels in key setup, needing only 1.5 encryptions and offering various options. It can be optimized for either fast encryption or quick key setup, making it suitable for encrypting large texts with a single key or encoding short blocks with frequently changing keys.

In every optimization method, accurately assessing the fitness of a solution is pivotal for determining the most optimal outcome. This fitness metric is established by taking into account both normalized variance and conditional privacy, expressed as Fitness Value = (NV + PR) / 2. Here, NV represents the normalized variance, which gauges the spread between original and altered data sets. Meanwhile, PR stands for conditional privacy, which evaluates the level of privacy of the original data (D) when compared to the altered data (E), calculated using the entropy function H with the formula P = 2H(D|E).

The established BEPO method is utilized for discovering the optimal secret key which is required for encrypting data designated for outsourcing to the CSP. The technique solution encoding is employed to visually depict the solutions, specifically the keys. Figure 3 demonstrates the encoding method which used in the proposed algorithm. This is employed to govern the most appropriate key to encrypt the medical data by considering the size as 1 × KZ.

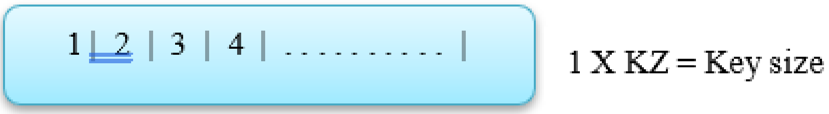

Figure 3. Encoding process of the Proposed method

3.3.5 Decryption

The decryption process will occur on the user's end. To access the actual content, the received data needs to be decrypted, which follows the same process as encryption, but in reverse.

4. FINDINGS AND EVALUATION

This part explains how we set up our experiment and what we found. We compared our expected method with some other methods called trust-based maxim and multilevel fair resource allocation. The performance is evaluated through various metrics such as attacks, false positive and false negative rates, the CPU usage in terms of number of cycles, overall execution time and detection rate. Our goal is to attain privacy efficiency while ensuring system compatibility with minimal error rates and execution times, and maximizing success rates. Additionally, graphical representations are employed to compare the proposed outcomes with the current technique.

The blockchain serves as a storage solution for patient information, encompassing details like patient name, age, gender, location (address), date of visit, and diagnosis he or she has undergone. Within each block, one finds the pertinent data alongside an index, nonce, previous hash, and timestamp. Utilizing a MATLAB program within an initial simulation model, we generated blocks and executed associated tasks such as adding new blocks and resolving challenges. Our investigation delved into the impact of escalating volumes of medical records within providers' databases on response time and throughput, across varying record counts. Notably, the system's throughput remains consistent despite heightened queries or stored records. This steadfastness underscores the system's adeptness in managing and processing extensive datasets swiftly and with minimal delay, akin to traditional MRs systems.

Regarding the process of Key generation, the Twofish with BEPO Key Generation technique was devised to bolster data security for information exchanged within cloud environments. This section assesses the effectiveness of the developed method using diverse performance metrics. The Twofish with BEPO Key Generation strategy for guaranteeing data security in the cloud is executed within the Python environment and subsequently simulated using CloudSim.

The evaluation metrics encompass various aspects of the Twofish with BEPO Key Generation technique's efficiency, including the amount of memory it occupies, time taken for validation, normalized variance value, and conditional privacy. Memory usage quantifies the amount of memory which is measured in terms of bytes required. Time taken for validation signifies the duration between receiving a user request and authentication. The metric, normalized variance value talks about the diffusion between real and distressed data. It is computed through statistical variance. Lastly, conditional privacy metric evaluates the privacy of actual data (D) compared to disturbed data (E), utilizing the entropy function (H) to determine the extent of privacy preservation.

5. CONCLUSION

In summary, integrating cloud computing into the healthcare sector offers significant advantages but also introduces vulnerabilities in data privacy. The proposed BPPRH system, which relies on Blockchain technology for privacy preservation and robust healthcare data management, faces risks such as ransomware, insider attacks, and malware injection during data transfer and storage. To address these challenges, the MFPSO method is introduced, aiming to optimize load distribution among virtual machines and utilize Edge Cloud based Collaborative Systems to enhance cybersecurity cooperation. Graphical representations of evaluations demonstrate notable performance enhancements, indicating the effectiveness of the proposed methods in securing healthcare data in the cloud. Additionally, a new data protection approach is suggested, leveraging the Twofish with BEPO Key Generation technique to ensure secure data transmission in the cloud. Through metrics analysis, including amount of memory consumed, time taken for validation, normalized variance value, and conditional privacy, the approach's effectiveness is showcased across various domains beyond healthcare. Future efforts will focus on enhancing security by integrating blockchain technology and refining encryption processes. Case studies will be conducted to assess the scalability and adaptability of the proposed methodologies in diverse cloud environments.

6. REFERENCES

[1] R. Ranchal, P. Bastide, X. Wang, A. Gkoulalas-Divanis, M. Mehra, S. Bakthavachalam, H. Lei, and A. Mohindra, I.E.E.E. J. Biomed. Health Inform. 24/11, 3182–3188 (2020). https://doi.org/10.1109/JBHI.2020.3001518.

[2] A. D. Dwivedi, et al., Sensors (Basel) 19/2, 326 (2019). https://doi.org/10.3390/s19020326.

[3] R. Sivan and Z. A. Zukarnain, “Security and privacy in cloud-based e-health system,” Symmetry, vol. 13, no. 5, p. 742, 2021 [doi:10.3390/sym13050742].

[4] O. A. Wahab et al., “Optimal load distribution for the detection of VM-based DDoS attacks in the cloud,” IEEE Trans. Serv. Comput., vol. 13, no. 1, pp. 114-129, 2017 [doi:10.1109/TSC.2017.2694426].

[5] H. Hamzeh et al., “MLF-DRS: A Multi-level fair resource allocation algorithm in heterogeneous cloud computing systems” in Conference on Computer and Communication Systems (ICCCS) 316–321, I. E. E. E. 4th International, Ed., 2019 [doi:10.1109/CCOMS.2019.8821774].

[6] D. C. Nguyen, et al., “Blockchain for secure EHRS sharing of mobile cloud-based e-health systems,” IEEE Access, vol. 7, pp. 66792-66806, 2019 [doi:10.1109/ACCESS.2019.2917555].

[7] N. Zainuddin, et al., “Risk evaluation using nominal group technique for cloud computing risk assessment in healthcare,” Int. J. Adv. Sci. Eng. Inf. Technol., vol. 10, no. 1, pp. 106-111, 2020 [doi:10.18517/ijaseit.10.1.10169].

[8] S. Sahar, et al.: Improved many-objective particle swarm optimization algorithms for scientific workflow scheduling in cloud computing, Ind. Eng. 147, 10664 (2020).

[9] S. R. Sheeba, et al., “Optimal users-based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers,” Multimedia Tool. Appl., 1-25 (2019).

[10] S. P. Kumar et al., “SLA-based healthcare big data analysis and computing in the cloud network,” J. Parallel Distrib. Comput., vol. 119, pp. 121-135, 2018.

[11] M. A. Almaiah, F. Hajjej, A. Ali, M. F. Pasha, O. Almomani, Sensors (Basel) 22/4, 1448 (2022). https://doi.org/10.3390/s22041448.

[12] A. Mehmood, et al., “Anonymous authentication scheme for smart cloud-based healthcare applications,” IEEE Access, vol. 6, pp. 33552-33567, 2018 [doi:10.1109/ACCESS.2018.2841972].

[13] S. Hu et al., “Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data,” IEEE Trans. Image Process., vol. 25, no. 7, pp. 3411-3425, 2016 [doi:10.1109/TIP.2016.2568460].

[14] B. Seth, S. Dalal, V. Jaglan, D. N. Le, S. Mohan, and G. Srivastava, Trans. Emerg. Telecommun. Technol. 33/4, e4108 (2022). https://doi.org/10.1002/ett.4108.

[15] H. Qiu, et al., I.E.E.E. J. Biomed. Health Inform. 24/9, 2499-2505 (2020). https://doi.org/10.1109/JBHI.2020.2973467.

[16] A. Rawashdeh et al., “An anomaly-based approach for DDoS attack detection in the cloud environment,” Int. J. Comput. Appl. Technol., vol. 57, no. 4, pp. 312-324

[17] V. Goyal and C. Kant, “An effective hybrid encryption algorithm for ensuring cloud data security” in Big Data Anal. Singapore: Springer, pp. 195-210, 2018.

[18] S. Namasudra, “An improved attribute-based encryption technique towards the data security in cloud computing,” Concurrency Compute. Pract. Experience, vol. 31, no. 3, p. e4364, 2019 [doi:10.1002/cpe.4364].

[19] I. Wagner and D. Eckhoff, “Technical privacy metrics: A systematic survey,” ACM Comput. Surv., vol. 51, no. 3, pp. 1-38, 2019 [doi:10.1145/3168389].

[20] B. Pushpa, “Hybrid data encryption algorithm for secure medical data transmission in cloud environment,” in Fourth International Conference Computing Methodologies and Communication (ICCMC), Erode, India, vol. 2020. IEEE, 2020, pp. 329–334. doi: 10.1109/ICCMC48092.2020.ICCMC-00062.

[21] Boumezbeur, I. & Zarour, K. (2022) Privacy-preserving and access control for sharing electronic health record using blockchain technology. Acta Informatica Pragensia, 11, 105–122. DOI: 10.18267/j.aip.176.

[22] S. Xie, F. Zhang, and R. Cheng, “SecurityEnhanced RFID authentication protocols for healthcare environment,” Wirel. Personal Commun., 1–16 (2020).

[23] Y. Cao, Y. Sun, and J. Min, Meas. Control 53/7–8, 1286–1299 (2020). https://doi.org/10.1177/0020294020926636.

[24] R. Zou, X. Lv, and J. Zhao, Inf. Process. Manag. 58/4 (2021). https://doi.org/10.1016/j.ipm.2021.102604.

[25] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, I.E.E.E. Access 7, 66792–66806 (2019). https://doi.org/10.1109/ACCESS.2019.2917555.

[26] S. P. Kumar, S. K. Mohapatra, and S. L. Wu, J. Parallel Distrib. Comput. 119, 121–135 (2018).

[27] M. Elhoseny, G. Ramirez-Gonzalez, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, I.E.E.E. Access 6, 20596–20608 (2018). https://doi.org/10.1109/ACCESS.2018.2817615.

[28] F. Thabit, S. Alhomdy, and S. Jagtap, Int. J. Intell. Netw. 2, 18–33 (2021). https://doi.org/10.1016/j.ijin.2021.03.001.

[29] Maddila Suresh Kumar and Vadlamani Nagalakshmi, Cluster Computing, 1275-1291, Vol 27, issue 2, 2024. https://doi.org/10.1007/s10586-023-04011-z.

[30] Maddila Suresh Kumar and Vadlamani Nagalakshmi, Journal of Information and Knowledge Management, Vol 23, issue 1, 2024.
https://doi.org/10.1142/S0219649223500624.