Recent Developments in Electronics and Communication Systems
KVS Ramachandra Murthy et al. (Eds.)
© 2023 The authors and IOS Press.
This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License 4.0 (CC BY-NC 4.0).
doi:10.3233/ATDE221238

Health Information Sharing in Cloud Environment Using Modular Encryption Standard

R.Sathya Prabha, K.Kanagasabapathi, K.Sajeeth, M.Aishwarya
Department of information technology, Dr.Mahalingam College of Engineering and Technology, Pollachi,India
sathyaprabha1250@gmail.com

Abstract. Despite the Cloud Environment's (CE) numerous and obvious improvements in healthcare, these issues continue to impede CE's development. In order to fully understand and utilise such issues, the utmost serious thinking is required. Global, national, and local health information are in demand. Setting up the required security protocols for handling security issues and breaches is essential for getting the most out of healthcare services. The Modular Encryption Standard (MES) is therefore being investigated for this research in order to provide requirement-based health data protection in light of the tiering of security efforts. According to the presentation evaluation, the suggested work outperforms other regularly used calculations against the security of health data in the CE environment in terms of enhanced performance and practical subjective security ensuring approaches.

Keywords. Cloud Environment, Security, Files, Modular Encryption Standard.

1. Introduction

The rapid development of networks, wireless medical sensors, advanced processing methods, and communication technologies has made modern medical systems conceivable. In this approach, massive amounts of health records are typically outsourced and held by outside parties like cloud service providers (CSP). There are serious security and privacy concerns with cloud services since CSPs are unreliable and could accidentally reveal users' sensitive data to unauthorised users. Smart technology like cell phones and computers are quickly taking over human existence as a convenient and alluring mode of communication that is not constrained by space or time. Through adaptable programmes like Google Applications and iPhone applications, which run on distant servers and take advantage of remote availability to the business, smart device users can access a wealth of information about various organisations. The coordination of dispersed computing via mobile devices is referred to as a "cloud environment" (CE) [1-4]. Although CE can offer a number of significant benefits, such a longer battery life and a high level of level storage capacity, its adaptability, flexibility, and a few crucial requirements remain to be significant barriers. It displays the CE structure. One of the main concerns is combining the security and protection of sensitive data. Although cloud-based health monitoring is currently of

tremendous interest to CE, it is not receiving the attention it deserves due to a lack of actual security. These steps should be made to convince a range of cloud clients to utilise cloud environments. Health information security (HIS) is an iterative technique that undergoes innovative adjustments as medical care contexts develop. In light of the change to new plans, think on the efficacy and applicability of HI's security systems and procedures. Since it is challenging to detect the hazards and gather the HI, small medical facilities must be utilised. This inquiry is aimed to help the trainer be ready for those requests and challenges so they can complete a thorough risk assessment and provide the appropriate security measures to ensure HI security. For flexible electronic administrations, CE is one option. On the other hand, the cloud environment will probably be an excellent way to examine the medical services sector. For patients and gatekeepers, CE provides new organisational structures and workplaces[5-9].

A. Related Work

The section provides a comprehensive overviewof the HI security threats and solutions for ensuring its privacy in the cloud. Extreme security and protection risks, as well as CE risks, have emerged as major concerns. CE's clients and ventures rely heavily on the types of help they provide. Various exploration endeavors and arrangements have been proposed to go to protection and security challenges [10-13].

Tele-observing is widely used to monitor a patient's health from a distance in settings like hospitals and crisis centres. There is a sizable E-health administration today. The identification, assessment, and treatment of the patient all make advantage of advancements in media transmission. Access to electronic health information is necessary for both making decisions and providing therapy (EHI). Even while EHI cloud-based monitoring and maintenance are growing in popularity, there are certain security concerns. An attempt at data theft is a crucial test among these challenges [14-19].

The cutting-edge technology known as cloud computing may totally transform the medical care sector. Adaptability, cost and energy investment funds, asset sharing, and rapid deployment are a few benefits of distributed computing. We focus on a variety of cloud security and protection issues in this study, as well as the use of distributed computing in the medical services sector. Patients and healthcare professionals alike should be concerned about their security and privacy due to the accumulation of data in the cloud. People and healthcare professionals therefore have total control over sensitive information. Attackers can gather information, capture information, and transfer ownership of information to co-ops with expertise in the cloud thanks to information centralization. Because of this, widespread adoption of the cloud is being held back by worries about security, privacy, productivity, and flexibility [20-22]. In this attempt, we found that the handicraft arrangements' existing state only meets a portion of the requirements that are worrying us; a comprehensive arrangement that takes into account all the competing criteria is urgently needed [23-26].

The Internet of Things (IoT) is growing in popularity. Massive volumes of data are produced by IoT devices. Investigation into the information produces a lot of information that could be quite helpful for IoT applications. IoT applications have new needs, such as mobility, continuous reaction, and space mindfulness, in contrast to conventional applications. Examples include attentive medical treatment, astute navigation, and ecological observation. The typically dispersed computing viewpoint, however, is unable to meet these expectations because of concentrated handling and being separated from neighbouring devices. Edge computing is more efficient and

environmentally friendly than scattered computing since it manages information processing and capacity closer to the edge of organisations. Sadly, edge registration poses serious security and protection risks when used for information inspection. The text actually doesn't give a full examination of the most recent advancements in secure information inquiry at the edge processing. In this work, we first present the idea of edge processing and its essential components. Then, by analysing potential security hazards in edge registering, we give a number of prerequisites for its reliable information evaluation. [27-29]

A generalised cloud computing record sharing strategy using attribute-based encryption has been implemented for financial institutions (ABE). Financial institutions must now deal with a security challenge due to a rise in data leaks, though, unless attribute-based encryption is utilised to safeguard the data. Searching through encrypted cloud data is really difficult. Use a hash-based searching technique to gain access to the encrypted data kept in the cloud. This strategy also recommends linking financial institutions with a third-party application. The implementation run and analysis show that the suggested solution outperforms existing security measures in terms of effectiveness and security. [30] If attribute-based encryption is not used to safeguard the data, there will be a rise in the amount of data leaks. In encrypted cloud data, searching is exceedingly challenging. To access the encrypted data stored in the cloud, one should use a hash-based searching method. Additionally, this approach suggests integrating a third-party application with financial institutions. The proposed approach is extremely effective and secure when compared to current security approaches, according to the implementation run and analysis. [30].

2. PROPOSED Methodology

Proposed Methodology

Utilizing the Modular Encryption Standard is the preferred architecture (MES). The Identification and Classification representation coordinates the requirement for obtaining HI (according to the degree of secrecy of HI). In this case, the recognisable proof would be obtained (to recognise the criticality and affectability of HI). The CE customer's feature must be what determines how to identify health records. Therefore, it usually includes two broad descriptors and sub-groupings. Open/public and secret H (with high-level security). In this section, the proposed project's outline is presented. the practises that must be adhered to in addition to MES to ensure HI privacy at CE. These six processes are carried out in part by the CE client; the remaining classification assurance procedures are carried out by the intermediary cloud (i.e., Crypto-cloud); and, finally, the data is stored using a multi-cloud. The suggested MES uses the CP-ABE as the executed computation.

These precautions are crucial for defending HI against insider and pariah assaults on the cloud given the nature of the stored data. The significant choice is based on the recognised evidence and categorization by HI. The wellness data would currently be (approximately) encrypted in the following module using the project worker/extender plot. This would complete the recognition of plaintext based on 56 bits and its expansion to 64 bits (i.e., light encryption). The project worker/extender plot is used to transfer it to the arbiter cloud, sometimes referred to as the crypto-cloud. This approach

prevents data from being given to the CSP without guarantees (i.e., in authentic plaintext structure anyway rather the drawn-out variant).

2.1 Modules

a) Group member registration and login:

The principal User chose any collecting id and entered his username and secret phrase in this module before registering with the Data Cloud Server. Gathering mark conspiracies allow any member of the gathering to sign messages, keeping the signer's identity a secret from verifiers. Furthermore, the mark's creator's identity may be revealed to the selected gathering administrator during a disagreement, which is meant to improve detectability. In this instance, the owner name and password are needed to create an owner login. In the user registration section, information about the user, including the user name, password, occupation, medical specialisation, and organisation, is kept. A user id is generated after user registration.

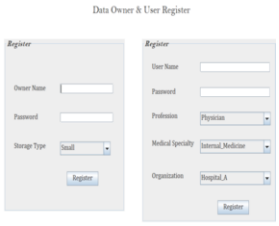

Fig.1 Registration

Fig.2 Login

2.2 Key Variances Based Analysis:

The numerous key types or key variations for these various plans are contained in this module (in accordance with the instructions provided by the customer for obtaining a certain level of security). This subjective method is similar. Using a single type of key, DES, 3DES, RC5, RC6, Blowfish, and IDEA all function without the need for any prerequisite-driven techniques. AES offers three types of keys (High level of necessity driven methodology). As a result, it is clear from the graph below that MES has the greatest number of significant important modifications.

2.3Batch Level Sign Based Key Generation:

Throughout the Key Generation module, every client in the group produces both their public key and private key. A client creates a private key and public key using an arbitrary p. Computerized marking makes use of imbalanced cryptography. The beneficiary of communications received across an uncertain route is encouraged to accept the message supplied by the guaranteed sender by a properly implemented advanced mark. Despite the fact that computerised marks resemble traditional handwritten marks in many respects, well-finished advanced marks are more challenging to produce than those that are transcribed.

2.4 Flow Diagram

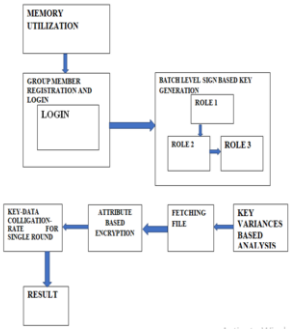

Figure.3 Flow Diagram

3.Results AND DISCUSSION

3.1 Modular Encryption Standard

This section offers the MES analysis in the cloud setting from a number of angles. The cloud-based MES installation follows these standards. The results of the performance analysis of our proposed work are shown in this section. We looked at the performance analysis capabilities of MES individually and in relation to other well-liked block cyphers for encryption. The MES has an O spatial complexity (n). It has been demonstrated that MES outperforms other popular algorithms in terms of low memory and CPU utilisation, as well as low processor utilisation, memory consumption, key variances, and data collation rate, making it a superior choice for smart devices (i.e., energy and resource-constrained devices). The developed method can deliver respectable outcomes in the cloud environment because it is supported by additional high-quality security assuring techniques.

3.2 Form Execution

a)Storing a file:

After registering, the file's owner has the ability to review patient data, store patient data in the cloud, and set access restrictions for the file.

After registering, the owner looks over the file and stores it. There is a browse button on the window that you can use to select the patient's file that needs to be saved. The owner selects the file and then clicks the store button.

b)Adding access Policy:

The owner makes the Access Policy available to the user in order to ensure the security of the shared file. The access policy window has a file selection box, a profession field where the user may choose their profession, a field where they can choose their medical specialty, and a field where they can choose the organisation.

If the file has been inappropriately accessed by any kind of user, the message will show up in the window as shown in the picture.

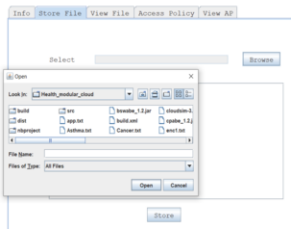

Figure 4. Storing a file

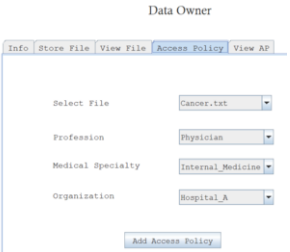

Figure 5. Adding Access Policy

Figure 6. Invalid Access Policy

4. CONCLUSION

- Security and protection issues are the major barriers to CE acceptance in the medical field. One of the more spectacular exploration holes is this one. In a manner similar to that, this research uses layered, private, information-nature-driven cryptography techniques, such as MES, which uses secure HI sharing and capacity tools. Comparative outcomes demonstrate that this approach outperforms other popular tactics in the CE environment (from many execution elements). The following highlights a few probable roadblocks and results of the suggested endeavour.
- Currently, there are no plans to collect data using this technology for image-based data gathering; rather, it is meant to analyse and translate text-based data. But when making new stuff, this problem will be taken into mind.
- Quantum registering in combination can improve the efficiency of the proposed task and make it more appropriate for mobile and smart devices. In the future, we could be able to ensure patient safety by utilising the blockchain security paradigm.

REFERENCES

[1] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, "eHealth cloud security challenges: A review," J. Medical care Eng., vol. 2019, Sep. 2019, Art. no. 7516035.
[2] H. Jin, Y. Luo, P. Li, and J. Mathew, "A survey of secure and protection saving clinical information sharing," IEEE Access, vol. 7, pp. 61656–61669, 2019
[3] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A study on secure information investigation in edge registering," IEEE Internet Things J., vol. 6, no. 3, pp. 4946–4967, Jun. 2019.
[4] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and protection safeguarding difficulties of E-wellbeing arrangements in distributed computing," IEEE Access, vol. 7, pp. 74361–74382, 2019.
[5] Algarni, "An overview and characterization of safety and protection research in keen medical services frameworks," IEEE Access, vol. 7, pp. 101879–101894, 2019.
[6] X. Wang and Z. Jin, "An outline of portable distributed computing for inescapable medical services," IEEE Access, vol. 7, pp. 66774–66791, 2019.
[7] C. Iwendi, S. Ponnan, R. Munirathinam, K. Srinivasan, and C.- Y. Chang, "A productive and remarkable TF/IDF algorithmic model-based information examination for taking care of utilizations with enormous information streaming," Electronics, vol. 8, no. 11, p. 1331, Nov. 2019.
[8] S. Kutia, S. H. Chaudhary, C. Iwendi, L. Liu, W. Yong, and A. K. Bashir, "Socio-mechanical elements influencing User's reception of eHealth functionalities: A contextual investigation of China and Ukraine eHealth frameworks," IEEE Access, vol. 7, pp. 90777–90788, 2019.
[9] N. A. Azeez and C. V. der Vyver, "Security and protection issues in E-wellbeing cloud-based framework: A complete substance investigation," Egyptian Informat. J., vol. 20, no. 2, pp. 97–108, Jul. 2019.
[10] S. Mbonihankuye, A. Nkunzimana, and A. Ndagijimana, "Healthcare information security innovation: HIPAA consistence," Wireless Commun. Versatile Comput., vol. 2019, Oct. 2019, Art. no. 1927495.

[11] M. G. Padmashree, S. Khanum, J. S. Arunalatha, and K. R. Venugopal, "SIRLC: Secure data recovery utilizing lightweight cryptography in IoT," in Proc. IEEE Region 10 Conf. (TENCON), Oct. 2019, pp. 269–273.
[12] R. Saha, G. Kumar, M. K. Rai, R. Thomas, and S.- J. Lim, "Privacy guaranteed E-medical services for mist improved IoT based applications," IEEE Access, vol. 7, pp. 44536–44543, 2019
[13] K. Edemacu, H. K. Park, B. Jang, and J. W. Kim, "Privacy arrangement in communitarian eHealth with characteristic based encryption: Survey, difficulties, and future bearings," IEEE Access, vol. 7, pp. 89614–89636, 2019.
[14] R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang, and Z. Wang, "Flexible and effective blockchain-based ABE conspire with multi-expert for clinical on request in telemedicine framework," IEEE Access, vol. 7, pp. 88012–88025, 2019
[15] X. Li, X. Huang, C. Li, R. Yu, and L. Shu, "EdgeCare: Leveraging edge processing for community information the executives in versatile medical care frameworks," IEEE Access, vol. 7, pp. 22011–22025, 2019.
[16] M. U. Sarwar and A. R. Javed, "Collaborative medical care plan through publicly support information utilizing encompassing application," in Proc. 22nd Int. MZultitopic Conf. (INMIC), Nov. 2019, pp. 1–6.
[17] V. Vijayalakshmi and L. Arockiam, "Hybrid security strategies to ensure delicate information in E-medical services frameworks," in Proc. Int. Conf. Shrewd Syst. Creative Technol. (ICSSIT), Dec. 2018, pp. 39–43.
[18] Y. Zhang, D. Zheng, and R. H. Deng, "Security and protection in savvy wellbeing: Efficient arrangement concealing trait-based admittance control," IEEE Internet Things J., vol. 5, no. 3, pp. 2130–2145, Jun. 2018.
[19] Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure personality-based information sharing and profile coordinating for portable medical care interpersonal organizations in distributed computing," IEEE Access, vol. 6, pp. 36584–36594, 2018
[20] Masood, Y. Wang, A. Daud, N. R. Aljohani, and H. Dawood, "Towards keen medical care: Patient information protection and security in sensor-cloud framework," Wireless Commun. Versatile Comput., vol. 2018, Nov. 2018, Art. no. 2143897.
[21] Anju Markose, Shebin Sharief, J Ramprasath, N Krishnaraj, “Survey on Application of IoT and its Automation”, International Journal of Advanced Engineering Research and Science, Volume 8, Pages 6, 2021.
[22] J Ramprasath, Dr. S Ramakrishnan, P Saravana Perumal, M Sivaprakasam, U Manokaran Vishnuraj, "Secure Network Implementation using VLAN and ACL", International Journal of Advanced Engineering Research and Science, Vol-3, Issue-1, pp. 2349-6495, 2016.
[23] J Ramprasath, M Aswin Yegappan, Dinesh Ravi, N Balakrishnan, and S Kaarthi, "Assigning Static Ip Using DHCP in Accordance with MAC", International Journal for Trends in Engineering & Technology, Vol. 20, Issue 1, 2017.
[24] J Ramprasath, V Seethalakshmi, “Mitigation of Malicious Flooding in Software Defined Networks Using Dynamic Access Control List”, Wireless Personal Communications, Vol. 121, pp. 107-125, 2021.
[25] P Jayasri, A Atchaya, M Sanfeeya Parveen, J Ramprasath, “Intrusion Detection System in Software Defined Networks”, International Journal of Advanced Engineering Research and Science, Volume 8, Issue 8, 2021.
[26] P Ramprakash, M Sakthivadivel, N Krishnaraj, J Ramprasath, “Host-based Intrusion Detection System using Sequence of System Calls”, International Journal of Engineering and Management Research, Vandana Publications, Volume 4, Issue 2, pp. 241-247, 2014.
[27] Ramprasath J, Seethalakshmi V, “Improved Network Monitoring Using Software-Defined Networking for DDoS Detection and Mitigation Evaluation”, Wireless Personal Communications, 116, pp. 2743–2757, 2021.
[28] J Ramprasath, P Ramya, T Rathnapriya, "Malicious attack detection in software-defined networking using machine learning approach", International Journal of Advances in Engineering and Emerging Technology, 11 (1), pp. 22-27, 2020.
[29] Dr. M Balakrishnan, Dr. AB Christopher, Dr. AS Murugavel, J Ramprasath, "Prediction of Data Analysis ", Int. J. of Aquatic Science, Volume 12, Issue 3, pp. 2755-2762, 2021.
[30] K Kanagasabapathi, S Balaji, “Secured Sharing of Financial Records with third party application integration in cloud computing”,International Conference on Current Trends in Engineering and Technology (ICCTET), July 2013.