Original Article

APPLYING THE MODULAR ENCRYPTION STANDARD TO MOBILE CLOUD COMPUTING TO IMPROVE THE SAFETY OF HEALTH DATA

M. Sunil Kumar[1], B. Siddardha[2], A. Hitesh Reddy[3], Ch.V.Sainath Reddy[4], Abdul Bari Shaik[5], Dr. D. Ganesh[6]

[1]Professor & Programme Head, Department of computer science and engineering

[2,3,4,5]School of Computing, Mohan Babu University, (erstwhile Sree Vidyanikethan Engineering College), Tirupati, AP, India

UG Scholar, Department of CSE, Sree Vidyanikethan Engineering College, Tirupati, AP, India.

[6]Associate Professor, Department of computer science and engineering, School of Computing, Mohan Babu University, (erstwhile Sree Vidyanikethan Engineering College), Tirupati, AP, India

Email: sunilmalchi1@gmail.com

DOI: 10.47750/pnr.2022.13.S08.231

Abstract

Mobile Cloud Computing (MCC) has numerous and easily observable benefits in healthcare, but its growth is being hampered by protection and security concerns. The problem at hand calls for one's whole attention and seriousness if one is to grasp its scope and make good use of it. A global, territorial, and local effort is required to disseminate health information. To completely profit of the wellbeing administrations, it is significant to set up the requested security rehearses for the counteraction of safety breaks and weaknesses.

Keywords: Cloud Computing, Health Data, security, Mobile Cloud Computing.

1. INTRODUCTION

As registering advances have advanced rapidly, distributed computing has become increasingly popular through the use of web-based programs, services, data storage, and computation. It finds widespread application in fields as diverse as medicine, agriculture, business, and information technology. It also motivates organizations who are adept at decoupling and providing _edible access to their assets. Shrewd gadgets like cell phones and tablets are dynamically transforming into an essential constituent of human existence as a helpful and compelling instrument for correspondence that isn't restricted by spot and time. Savvy gadget clients gather rich experience of various organizations from versatile applications, for example, Organizations can benefit from Google Apps and iPhone Apps that are hosted on remote servers and accessed by employees from within the company. "Mobile Cloud Computing" refers to the use of mobile devices for coordinating distributed computing (MCC).As MCC can offer a couple signi_cantbene_ts, for instance, extended battery life and significant level stockpiling ability, versatility, flexibility, and a couple of key requests continue to be a signi_cant deterrent to MCC. An outline of MCC is portrayed. One of the main challenges consolidates the security and protection of secret data[19][20].

Reevaluate HI's security setup and procedures in light of forthcoming plans to revamp the system's quality and sufficiency. Perceiving the dangers and getting the HI is testing and requesting for little wellbeing places[9]. This exploration is planned to empower the training to prepare for those requests and difficulties, for powerful danger evaluation, and give appropriate security ways to deal with guarantee HI safety[23]. For flexible electronic administrations, MCC is a feasible approach. Similarly, MCC seems like it will be a great method to screen the healthcare industry. Healthcare providers and patients alike can benefit from MCC's innovative organizational structures and working environments[21][24].

1.1 MOBILE CLOUD COMPUTING

In order to provide rich computational resources to mobile clients, network administrators, and distributed computing service providers, Mobile Cloud Computing (MCC) combines distributed computing with portable registration[17]. One of MCC's

main goals is to facilitate the deployment of feature-rich, cross-platform apps to a large number of mobile devices. Similar to cloud service providers, MCC allows for greater administrative flexibility within an enterprise[27][7]. More comprehensively, MCC is "a rich handheld registering innovation that use gathered together versatile assets of different mists and organization breakthroughs toward unchallenged helpfulness, stocking up, and flexibility. In most contexts, this word refers to a large number of servers that can serve as a resource to a wide range of users across the Internet. Today's enormous, transcending mists often have capabilities that are dispersed across different locations from central servers. The client may be directed to an edge server if its connection to the network is relatively fast[25][28].

Mists may be available to multiple organizations (general mists), or they may be exclusive to a single organization (undertaking mists) (public cloud). Using shared resources is essential for distributed computing to achieve awareness and scale efficiently[26]. Distributed computing, say proponents of public and hybrid clouds, helps businesses avoid or significantly reduce the need for costly up-front investments . Since most cloud service providers operate on a "pay-more just as costs emerge" basis, managers who are unfamiliar with cloud-evaluation methods may be caught off guard by unexpected growth in operational expenses[29].

1.2 REQUIREMENT-ORIENTED APPROACH

It is generally utilized from a proper perspective in designing plan, incorporating for instance in frameworks designing, computer programming, or endeavor designing. A wide idea could address any important (or in some cases wanted). Prerequisites can accompany various degrees of explicitness; for instance, a necessity detail or necessity "spec" (frequently loosely alluded to as "the" spec/specs, however there are really various kinds of particulars) alludes to an express, exceptionally evenhanded/clear (and regularly quantitative) necessity (or at times, set of necessities) to be fulfilled by a material, plan, item, or administration[8].

A bunch of prerequisites is utilized as contributions to the plan phases of item advancement. Prerequisites are additionally a significant contribution to the check interaction, since tests should follow back to explicit necessities[13][12]. Prerequisites show what components and capacities are essential for the specific undertaking. At the point when iterative techniques for programming improvement or lithe strategies are utilized, the framework prerequisites are gradually evolved in corresponding with plan and execution. With the cascade model necessities are created before plan and execution[11][14][16].

2. RELATED WORK

In this section, we have a look at the written summary of the risks to HI security and methods for ensuring its privacy in the cloud. There are now major concerns about the severe security and safety risks posed by MCC. The businesses and individuals who use MCC's services rely heavily on them. Multiple investigations and plans have been offered to address safety and security issues [30][32].

Protecting patients' identities and personal information is crucial in the healthcare industry. Because of recent technology developments, electronic health records have completely supplanted their paper predecessors (EHR)[17]. Everything, including medical records, has gone digital and mobile in recent years. Healthcare institutions put their patients' private information on network servers so that it may be accessed more easily. However, this has resulted in a number of data breaches as a result of security flaws[33].

2.1 Types of Threats in Healthcare:

Here are some examples of the various dangers the healthcare sector faces: Incidents using computers and the internet: They encompass anything from phishing to malware outbreaks. These account for the vast majority (70%) of all attacks[20]. Since reports of hacking events began in 2010, they have steadily increased. Software flaws are largely to blame for the prevalence of assaults. Various vulnerabilities in their security systems make them easy targets for cybercriminals. Fearing punishment and slander, many incidents went unreported. There were 9.1 million records reportedly exposed due to hacking and other IT issues[34][10].

Rising as more and more mobile devices, like smartphones and tablets, join the internet[22]. this includes a vast array of medical gadgets. The difficulties in ensuring the safety of information technology (IT) systems in the healthcare industry were explored

by Ahmed et al. [5]. Data collection, network collection, and storage are the three stages of an attack that Ahmed et al. [5] identified. Aging infrastructure, medical devices, a culture of security, and the need to comply with laws and regulations are cited as the key reasons why hospitals are such prime targets for criminals. In order to detect any form of malicious activity in the system or network, Ahmed et al. [5] employed Indicators of Compromise-based Metrics (IOC). When a company is hit by malware, it may be days or weeks before anyone realizes what happened. Indicator of Attack is a security measure mentioned by Ahmed et al. [5] for this purpose (IOA). This preventative step is implemented to expose an attack before the IOC identifies it. In addition, Ahmed et al.[5] detail six more metrics for thwarting cyberattacks. Risk assessment metrics include things like red and blue teaming effectiveness, vulnerability assessment effectiveness, penetration testing effectiveness, and intelligence-driven defense effectiveness. [5][35]

According to a study published in 2020 by Devi et al. [6], hackers frequently target healthcare organizations. Data breaches still occur despite firms' compliance with HIPAA regulations due to various security flaws. Instead, biometrics have been implemented to safeguard patient identity and authentication within the healthcare system, allowing for the mitigation of potential security risks[31]. In their analysis of the factors that lead to data breaches, Devi et al. [6] noted that criminal hackers take advantage of system weaknesses, The theft of a variety of computers belonging to healthcare personnel, Accidental data leaks due to user error, third-party integration failures, and technical errors all fall into this category. Biometrics have been discussed by Devi et al. [6], who point out their potential utility in reducing cyber-attacks in the healthcare sector. There are two main functions of the biometric authentication system: enrollment and authentication[18]. In Enrollment mode, the scanner scans the biometrics, which can be recognized using a pattern recognition system, when a valid user enrolls a finger. This is then used to create digital biometric templates for the healthcare database. When a medical professional requests access to a patient's records, the scanner will compare the scanned biometrics to those stored in the database in order to authenticate the user. If these biometrics are a match, the user is allowed in; otherwise, they are denied entry. [6][37][36].

The following [3] dangers pose the greatest danger to healthcare organizations and affect the greatest proportion of those institutions:

Sometimes, vulnerable OS could be a huge risk because the security flaws and vulnerabilities are already out there if the software is not updated. All these security vulnerabilities are stored in the databases such as exploitdb.com. To search for the vulnerabilities, all the hackers must do is search for CVE-year-number, (CVE is a security flaw assigned a CVE ID number). According to Allen Bernard [3], TechRepublic, 83% of the hospitals or any healthcare organizations are using outdated software [3][32]. Hence, keeping the software up to date could reduce the number of attacks. The medium risks and percentages of the healthcare organizations which are affected by these threats are [3]:

- Threat Percentage of Breaches
- Configuration vulnerabilities 60%
- Risky hotspots 56%
- Sideloaded apps 24%
- Crypto jacking 16%
- Third-party app stores installed 16%.

Fig 1 Ransom ware Attack Anatomy

3. PROPOSED METHODOLOGY

Specifically, the suggested architecture makes use of the Modular Encryption Standard (MES). IDN and CLF depiction of the importance of obtaining HI work in tandem with one another . Here is where the obvious proof would be carried out (to establish the importance and sensitivity of HI). The MCC client's highlighted needs determine the IDN of medical files. Two broad categories are typically included, with further subdivisions. Both open/public and secret HI are available. This section provides a high-level breakdown of the planned effort. How to balance the need to protect sensitive information (HI) while using the Management and Enterprise Services (MES) platform at MCC. Some of these six steps are completed on the client side of the MCC, with the rest of the categorization ensuring steps being taken in the intermediary cloud (i.e., Crypto-cloud) Last but not least, multi-cloud storage is used to archive the data. The suggested mes employs the CP ABE as the operationalized computation

These actions are vital to secure HI against the various types of assaults at the cloud i.e., insider's and pariah's assaults. in view of the kind of data put away. The key determination is reliant upon HI recognizable proof and characterization. Presently, the following module would encipher the wellbeing record (somewhat) using the project worker/extender plot. At this point, we'd have completed the decryption of 56-bit plaintext and its expansion to 64-digit (i.e., lightweight) encryption. Once the data has been processed by the project's workers and extenders, it is sent on to the arbiter cloud, also known as the crypto-cloud, for final resolution. In this manner, information is not given to the CSP without any assurances

3.1 MEMORY UTILIZATION

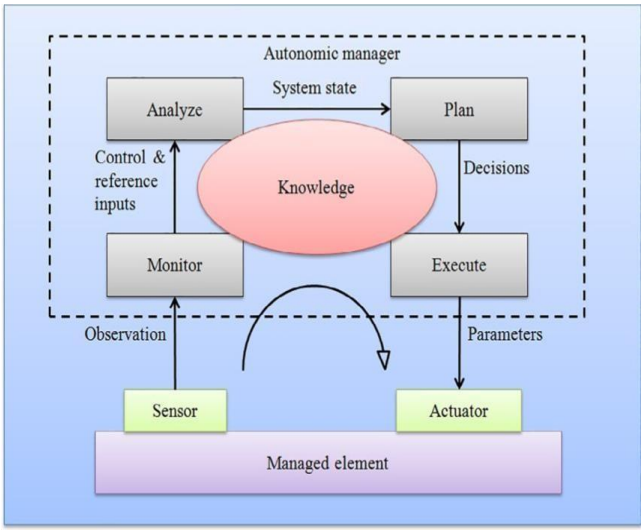


Fig 2. IoT Managed Element

Fig2.IoT Managed Element Registered proprietor can add the record in line with the entire length allotted on the time of registering. The Memory usage is the common usage derived from the percentage of to be had reminiscence in use at a given moment

3.2 KEY VARIANCES BASED ANALYSIS

In this module the forms of keys (in line with person-unique necessities for accomplishing a particular stage of security) or key versions of CP ABE Hence, it may be located that MES possesses the very best stage of key variances.

3.3 BATCH LEVEL CONDITION BASED ACCESSABILITY

In this module the facts proprietor will set the primary situations. The person who wishes to fetch the facts may be capable of get the facts best if the circumstance of the facts proprietor matched. The get admission to may be declined if the situations are mismatched.

3.4 CLOUD SETUP MODULE

This module complements the schemes which permit circumstance primarily based totally authentication and offer end result similarity rating for

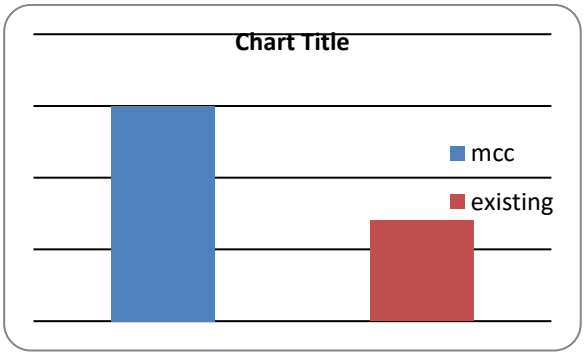
powerful facts retrieval, as opposed to returning undifferentiated results. Privacy-Preserving: To save you the cloud server from gaining knowledge of extra statistics from the uploaded facts and the index, and to satisfy privateness. Efficiency: Above desires on capability and privateness have to be finished with low conversation and computation overhead.

4. EVALUATION:

This module is used to assist the server to encrypt the file the use of CP ABE Algorithm and to transform file to the steady encrypted record with situations.

algorithm	efficiency
mcc	95
existing	87

It tends to be imagined that MES has preferred execution over other usually utilized calculations as far as low processor use rate, less memory usage, the most extensive level of key changes, and most elevated information colligation rate and this low memory and processor use settles on a more great decision for cell phones (i.e., energy and asset compelled gadgets). Because of the other unmistakable subjective security guaranteeing measures displayed, the planned plan can give OK outcomes in the MCC climate.



5. CONCLUSION

Despite MCC's future arrangements in Health information checking, a number of constraints constrain its crucial potential. In particular, safety and privacy concerns have been identified as significant roadblocks to the widespread adoption of MCC in healthcare. Among the many remarkable exploration holes, this one stands out. Similarly, this investigation makes use of a multi-tiered, isolated, information-driven cryptography technique, such as MES, which employs safe methods of exchanging personally identifiable information (PHI) and measuring resources. The comparative results demonstrate that in the MCC environment, this strategy outperforms other commonly used strategies (from a variety of execution aspects). Below, we list several potential roadblocks to the proposed work as well as its potential future directions.

To date, this approach has only been considered for the deciphering and translation of textual material; gathering data from visual sources is not even being considered. However, this concern will be taken into account in further projects. As a further downside, tiered demonstrating can occasionally result in reduced framework efficiency. Additionally, the proposed work's efficiency can be enhanced by reconciling quantum registration to make it more adaptable for mobile and clever devices. In the future, we may be able to ensure patient safety via a block chain-based security architecture.

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. Chauhdary, 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 HIoT," 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. 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.
17. Balaji, K., P. Sai Kiran, and M. Sunil Kumar. "Resource aware virtual machine placement in IaaS cloud using bio-inspired firefly algorithm." Journal of Green Engineering 10 (2020): 9315-9327.
18. Sangamithra, B., P. Neelima, and M. Sunil Kumar. "A memetic algorithm for multi objective vehicle routing problem with time windows." 2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE). IEEE, 2017.
19. Peneti, Subhashini, et al. "BDN-GWMNN: internet of things (IoT) enabled secure smart city applications." Wireless Personal Communications 119.3 (2021): 2469-2485.
20. Kumar, M. S., Ganesh, D., Turukmane, A. V., Batta, U., & Sayyadliyakat, K. K. (2022). Deep Convolution Neural Network Based solution for Detecting Plant Diseases. Journal of Pharmaceutical Negative Results, 464-471.
21. Ganesh, M. D., Tech, M., Kumar, M. S., & Prasad, V. R. (2016). IMPROVING NETWORK PERFORMANCE IN WIRELESS SENSOR NETWORKS. Integrated Intelligent Research (IIR), International Journal of Web Technology, 5(01), 58-61.
22. Sangamithra, B., Swamy, B. M., & Kumar, M. S. (2021). A comparative study on a privacy protection in personalized web search. Materials Today: Proceedings.
23. Davanam, Ganesh, T. Pavan Kumar, and M. Sunil Kumar. "Efficient energy management for reducing cross layer attacks in cognitive radio networks." Journal of Green Engineering 11 (2021): 1412-1426.
24. Natarajan, V. A., Tamizhazhagan, V., Tangudu, N., & Kumar, M. S. (2022). Analysis of Groundwater Level Fluctuations and its Association with Rainfall Using Statistical Methods. JOURNAL OF ALGEBRAIC STATISTICS, 13(3), 1895-1904.

25.Kumar, M. S., Harika, A., Sushama, C., & Neelima, P. (2022). Automated Extraction of Non-Functional Requirements From Text Files: A Supervised Learning Approach. Handbook of Intelligent Computing and Optimization for Sustainable Development, 149-170.
26. Kumar, M. S., Chandra, K. G., & Gupta, K. K. (2022). Stocks Analysis and Prediction of Indian Oil Trading Using Big Data Analytics. International Journal of Mechanical Engineering, 7(1), 6734-6738.
27. Natarajan, V. A., Kumar, M. S., Tamizhazhagan, V., & Chevdumoi, R. M. (2022). PREDICTION OF SOIL PH FROM REMOTE SENSING DATA USING GRADIENT BOOSTED REGRESSION ANALYSIS. Journal of Pharmaceutical Negative Results, 29-36.
28. Prasad, T. G., Turukmane, A. V., Kumar, M. S., Madhavi, N. B., Sushama, C., & Neelima, P. (2022). CNN BASED PATHWAY CONTROL TO PREVENT COVID SPREAD USING FACE MASK AND BODY TEMPERATURE DETECTION. Journal of Pharmaceutical Negative Results, 1374-1381.
29. Burada, S., Swamy, B.E.M., Kumar, M.S. (2022). Computer-Aided Diagnosis Mechanism for Melanoma Skin Cancer Detection Using Radial Basis Function Network. In: Kumar, A., Ghinea, G., Merugu, S., Hashimoto, T. (eds) Proceedings of the International Conference on Cognitive and Intelligent Computing. Cognitive Science and Technology. Springer, Singapore. https://doi.org/10.1007/978-981-19-2350-0_60
30. Dr. T. V. S. Gowtham Prasad*, Dr. B. Rama Rao, Dr. D. Nataraj & Srikanth Lammatha. (2022). Design of Multi Band Micro Strip Patch Antenna for S-Band and Ku Band Applications. Journal of Optoelectronics Laser, 41(6), 405–411. Retrieved from http://www.gdzjg.org/index.php/JOL/article/view/540.
31. T Ravi Kumar Naidu, M. Susila, T V S Gowtham Prasad, " Developments And Challenges In The Design Of Active Integrated Antennas ",Elementary Education Online, 16(1): 35-59 , 2021.
32. Ramu, M. M., Shaik, N., Arulprakash, P., Jha, S. K., & Nagesh, M. P. (2022). Study on Potential AI Applications in Childhood Education. International Journal of Early Childhood, 14(03), 2022.
33. Gurumurthy, S., Sushama, C., Ramu, M., & Nikhitha, K. S. (2019). Design and implementation of intelligent system to detect malicious Facebook posts using support vector machine (SVM). In Soft Computing and Medical Bioinformatics (pp. 17-24). Springer, Singapore.
34. M. U. Sarwar and A. R. Javed, "Collaborative medical care plan through publicly support information utilizing encompassing application," in Proc. 22nd Int. Multitopic Conf. (INMIC), Nov. 2019, pp. 1–6.
35. 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.
36. 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.
37. 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