International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 05 Issue 02 | 2021

A Secure G-Cloud-Based Framework for Government Healthcare Services

[1]Suresh Aneesh Jain, [2]Dr. Bhuvana J

[1]MCA Scholar, Department of MCA, Jain University, Bangalore
[2]Faculty MCA Scholar, Department of MCA, Jain University, Bangalore

ABSTRACT

Now –a-days cloud computing technology is a most used and demandable technology in the IT Environment. As per the Current requirements and demands in the health care system many to convert the system into the cloud environment to meet the future needs and fulfill the demands. In this paper, we propose a System with Secure, cost effective and flexible Government cloud-based Framework for the health care system. We propose a protected and effective system for the public authority Electronic health record, in which fine-grained admittance control can be managed the cost of dependent on multi-authority cipher text property-based encryption (CP-ABE), along with a various leveled structure, to uphold access control arrangements. This system intends to give wellbeing administrations and offices from the public authority to residents (G2C). Besides, multifaceted candidate confirmation has been distinguished and sealed in participation with two confided in specialists. Security investigation and correlations with the connected structures have been led.

Keywords - Cloud Computing, Electronic Health Record, Security, Attribute-based Encryption, Cipher text policy, Identity Proofing, Authentication, Authorization.

1. INTRODUCTION

A common development in tending in most Arab countries is that the lack of optimum utilization of human and material resources out there to produce integrated tending to stop diseases and treat diseases when they occur. Statistics indicate that Arab countries suffer from high rates of health issues, like polygenic disorder, disease, and parasitic diseases, like histaminases and protozoal infection. These health issues can be prevented before they occur or their complications prevented by early detection. This can be because of a mix of factors: coming up with, operational, and technical. If we have a tendency to were able to overcome them, this might cause vital progress within the level of health care. additionally, there's a weakness and lack of accessible hospital data systems, that is a few of the foremost advanced computer code that directly serves all technical and body tending activities, making certain that the health facility has full management over all its activities and resources. The successes of those advanced systems don't depend upon the precise choice of apparatus and computer code for storage. Rather, their success depends on their suitableness for various users—from tending suppliers, like doctors, nurses, technicians, and even administrators—where the vision and priorities of every of those classes dissent, and their data desires vary, as do the advantages of every of those systems.

The traditional health system (paper) has been replaced by Associate in Nursing electronic health system as a result of the standard system has been found to be ineffective because of variety of problems, as well as low storage capability, high operative and maintenance prices, and system integration. The computerized health system was then replaced by cloud computing as a result of it depends on a additional economical infrastructure, moreover because the several advantages of cloud computing in IT, like value, measurability, flexibility, and alternative options. The utilization of cloud computing in electronic health records reduces prices within the provision of health services, maintenance prices, networks, licensing fees, and infrastructure normally, and this can so encourage developers to adopt the cloud in tending.

The speedy shift to the cloud and its use in tending systems has raised considerations regarding crucial problems with privacy and data security .The adoption of the cloud in IT will increase the main focus and concern of tending suppliers on clinical and patient-related services and reduces attention on infrastructure management .The sharing of private and health data across the net and numerous servers outside the safe atmosphere of the tending establishment has semiconductor diode to variety of issues associated with privacy, security, access, and compliance problems. Within the literature, there are not any existing powerful frameworks that clearly address all viable schemes and interrelationships between cloud computing and tending technology. rising the framework for tending in cloud computing has been studied by many researchers. Additional developments and solutions in these challenges can increase the adoption of cloud tending and encourage tending suppliers to maneuver forward with cloud-based services.

2. LITERATURE SURVEY

[1] This paper purpose a solution for health care system by using the cloud computing and web services. With the use of the cloud computing, help in remote monitoring and controlling will be possible. It also provides an automatic update of measured parameters of patient and it also sends mail alert using Simple mail Transfer protocol(smtp). In this the sensor data will be sent to a gateway for monitor with a fixed Ip address and this proposed also provides an emergency alert signal if the condition of the patient is found critical and also if the data cross a threshold value it will send an emergency mail to a doctor. Using cloud computing and web service in the health care system provide a good solution, critical condition can be avoided by viewing in the webpage.

[2] Encryption is a good way to maintain the privacy of the data, but it makes a challenging task to maintain the confidentially. in this paper the author had focused on the problem of matching over outsourced encrypted datasets in identity-based cryptosystem that cam simplify the certificate management. To solve this problem the author has purposed a Identity based private scheme (IBPS) method, which fine grained authorization and enables the privileged cloud server to perform private matching operations without leaking any private data. The author had used a decisional linear Assumption and decisional bilinear, Diffie Hellman Assumption for the security. At last, we build IBMP on identity based fuzzy private matching scheme and an identity based multi key word fuzzy search scheme.

[3] Cloud computing security refers to protection of data in the cloud. Information and security of data storage, a part of cloud security aims to prevent the unauthorized use of the private data and modification of the data, when it happened it occurs a lot security concerns and the security of data is questionable. In this paper, the author proposed some cryptographic algorithms like RSA, AES and One Time pad. Where, the strong cryptographic algorithms are strong and unbreakable. In this paper, author compares the algorithms and find the strong data in the cloud. In last, after the comparison we found RSA and One Time pad (with variation) hold lesser complexity when compared to other hybrid models. Whereas AES takes more space, but One time pad takes space equal to its plain text, which makes that RSA and One time pad is efficient in terms of time, space complexity and the cipher text can’t be attacked easily.

[4] In this paper, the author designed an improved symmetric homomorphic cryptosystem and fog-based communication architecture to support time sensitive monitoring and other related applications, where as the medical data can be analyzing at a fog server in a secure manner. Here we present two attack methods to demonstrate that our approach is secure and evaluate the complexity of its computations. We also demonstrate that our schema satisfies key security properties and evaluating its performance using Microsoft azure.

[5] The data security and consumer data privacy are the challenges of the cloud era. The appropriate and privacy of data stored in cloud may be comprised because of limited security by owners of data. In this paper, the author presents an extensive survey of security in cloud. The security of the data is further analyzed in terms of data integrity, access control and attribute-based encryption. The author had proved a comparison table which indicates the security of data with the help of different methods. according to the table provide, it concludes that data and storage security should be provide with less storage and computational overhead.

[6] The e-healthcare management system could be increased with the extreme connecting to the technology. In this paper the author proposed a model of grouping adaptable e-healthcare service administration framework dependent on cloud computing. The model is dependent on disturbed computing. Here the entire patient data should require a focal database and cloud designs gives a web empowered system. With the end goal to deal with security and consistently developing the information to various clients, a cloud base bio metric validation framework, this model has two parts; one is administration level and second is security.

[7] The health care system can be improved by enhancing a new technology trend into the system. In this paper the author designs a model of flexible e-healthcare management system based on cloud computing system and service-oriented architecture (SOA). Cloud and SOA are becoming more use full nowadays. This system improved and includes different fractions to develop healthcare system, Rich Internet Application (RIA) based on the client side, simple database cloud server and application side leads to achieving reliable network. This model proposed improves cost management, time and storing profile and taking the right decision from the doctor.

[8] These papers consist of the electronic health record implementation process as well as application. With different backgrounds, each health institutions adopt different frameworks and also faces different challenges in the process which provides an impact of using the health care system more easily than the traditional system. [9] Cloud storage is a trending technology now a days, however data security, reliability, user privacy and other issues in the business can be decisive factors in application .in this paper, uses symmetric encryption in cloud storage to increase the security and also uses the hardware encoding method to encrypt before transmitting the data to the cloud and the data is difficult to crack after leaving the owner. In cloud storage, user information and data storage will be separated from each other to enhance the security and unauthorized services.

[10] Now a day’s technology sharing data with other now much confidential .so sharing of cloud based on mobile devices require some infrastructure to secure data over cloud. Cipher text policy attribute-based encryption is a technique which provides a fine-grained access to data over cloud but the Cipher text policy attribute-based encryption has a disadvantage with the key management, to overcome of this disadvantage, in this paper the author had proposed a collaborative key management protocol in Cipher text policy attribute-based encryption. In this, private keys are generated and stored in distributed manner and attribute revocation mechanism is provide for key update .it will minimize the problem of key exposure and decryption server is used to optimize user experience by minimize decryption load.

3. EXISITING SYSTEM

In 2010, Wang et al. projected a hierarchical attribute- based mostly coding (HABE) theme by combining the stratified identity-based coding system and therefore the ciphertext-policy attribute-based coding (CP-ABE) system. , then creating a performance-expressivity exchange, finally applying proxy re-encryption and lazy re- coding to their theme. In 2007, Bethencourt et al. Ciphertext-policy attribute-based coding (CP-ABE), collectively of the foremost promising coding systems during this field, permits the coding of information by specifying Associate in Nursing access management policy over attributes, so solely users with a group of attributes satisfying this policy will decipher the corresponding information.In 2013, Li et al. projected Associate in Nursing communicatory centrifugal KP-ABE theme. The ciphertext size doesn't think about the quantity of attribute employed in ciphertext. User's keys ar hooked up with access structures and ciphertext is related to attributes. A user is in a position to decipher, if ciphertext's attributes is that the licensed set of the access structure. In 2013, Li et al. increased a Multi-authority Attribute base coding (MA-ABE) theme to handle economical and on-demand user revocation, and prove its security. The projected MA-ABE theme utilised ABE to cipher and access not solely the patient information however conjointly varied users from property right with totally different skilled roles, qualifications and affiliations. In 2012, Alshehri et al. projected a cloud-based EHR system, that consists of the cloud-based information storage and computing resources, health care suppliers, and attribute authority (AA). during this theme, one single AA is answerable for key management, as well as generation, distribution, and revocation within the EHR system. The projected theme thought-about a CP-ABE theme and arranged EHR to the labeled stratified organisation to produce flexibility, quantifiability, and fine-grained access management.

4. PROPOSED SYSTEM

Provides a versatile, secure, cost-efficient, and privacy- preserved G-cloud-based framework for state health care services by Applying, using, and modifying the foremost recent secret writing and decoding mechanisms fitted to cloud-based EHR systems.

The projected theme doesn't use the quality secret writing system, that isn't suited to the cloud surroundings. Achieving quantifiability of computing resources that may be dilated and controlled in keeping with the desired health services. The EHR is ready to support huge information exchanges. o Providing a good resolution for call manufacturers within the government health sector to adopt cloud-based health care systems, particularly in developing countries. Providing an improved authentication multifactor human authentication in cooperation with two sure authorities. Different domains of attributes area unit managed by completely different attribute authorities, that operate severally from one another and controlled by the central sure authority. Security analysis has been conducted in keeping with major security needs in cloud environments.

4.1 Advantages of proposed system

- Apply for an identification number (ID) from the trusted authority to be able to access specific parts of the patient’s record which keeps data more secured.
- Apply a request for the secret key attached with the appropriate parameters.
- Be able to decrypt, modify, and encrypt the same document with the same key.

4.1.1 System Architecture

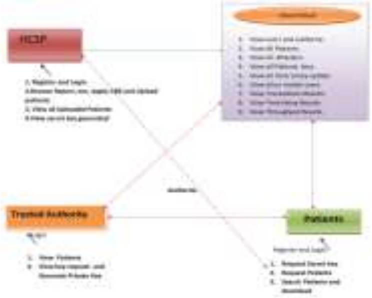

Fig 4.1.1 System architecture

4.1.2 Modules

- HCSP-In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the patients details and will do the following operations like Upload Patient Details, View All My Uploaded Patients, View Public Keys, View Transaction Details
- Patients-In this module, user logs in by using his/her user's name and password. After Login user requests search control to cloud and will Search for Patients have based on the index keyword with the Score of the searched Patient and downloads the Patient. User can view the search of the Patients and also do some operations like Search, Request Key, Request File, and View Keys
- EGovt Cloud Server -The cloud server manages a cloud to provide data storage service. Data owners encrypt their data Patients and store them in the cloud for sharing with Remote User and will do the following operations like View HSPs and Patients, View Patient Details, View Attackers, View Patient Keys, Un Revoke User, View Transaction, View Transactions Results, View Time Delay Results, View Throughput Results
- Trusted Authority-In this module, TA logs in by using his/her user's name and password. After Login he will do some operations like View all Patients, Generate Public Key Requests, key generation.

5. FLOW CHART

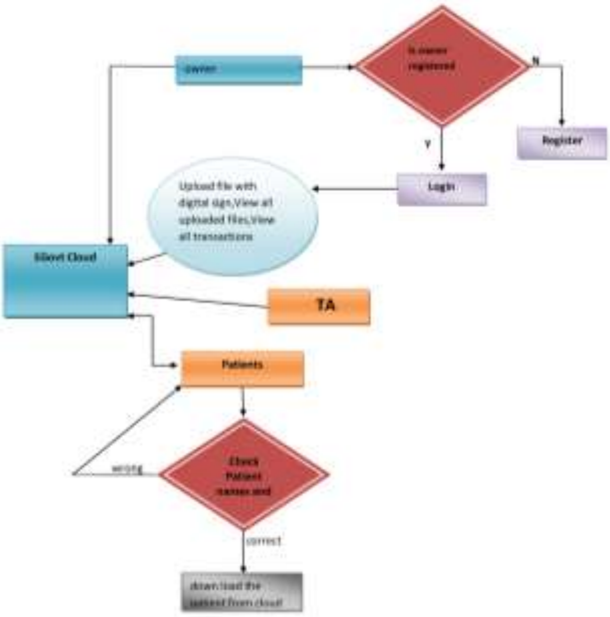
owner
Is owner registered
N
Register
Y
Login
Upload file with digital sign,View all uploaded files,View all transactions
EGovt Cloud
TA
Patients
wrong
Check Patient names and
correct
download the patient from cloud

Fig 6.1 flow chart

In the above flow chart, there are four entities they are HSP (hospital management), EGOVT, Trusted Authority, Patient. The hsp (hospital management) has a right to see the documents of patient which are stored in the Egovt which is a government cloud. The patient can have two logins one is new user and other is old user, so the patient will get his documents list which is uploaded by hsp and the patient can download the document but he needs an encryption key which he can request to TA (trusted authority), the trusted authority will accept the request of the file will generate the public key and send to the patient so the patient can copy the key and can view the document and download the file. The hsp has two logins one is old user and new registration.

7. CONCLUSION AND FUTURE ENHANCEMENT

In this, we have a tendency to projected a secure cloud-based EHR framework that guarantees the safety and privacy of medical information keep within the cloud, hoping on gradable multi-authority CP-ABE to enforce access management policies. The projected framework provides a high level of integration, ability, and sharing of EHRs among health care suppliers, patients, and practitioners. within the framework, the attribute domain authority manages a distinct attribute domain and operates severally. additionally, no machine overhead is completed by the govt. authority, and multi-factor mortal authentication are known and treated. The projected theme is adopted by any government that encompasses a cloud computing infrastructure and provides treatment services to the bulk of national patients. Future work includes implementing and evaluating the projected theme during a real-world setting.

8. REFERENCE

[1] Ghuge, M. and Chatur, P., 2018. Collaborative Key Management in Ciphertext Policy Attribute Based Encryption for Cloud. *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*.
[2] Dhanaliya, U. and Devani, A., 2016. Implementation of E-health care system using web services and cloud computing. *2016 International Conference on Communication and Signal Processing (ICCSP)*,
[3] Qiu, S., Liu, J., Shi, Y., Li, M. and Wang, W., 2018. Identity-Based Private Matching over Outsourced Encrypted Datasets. *IEEE Transactions on Cloud Computing*, 6(3), pp.747-759.
[4] Kodumru, N. and Supriya, M., 2018. Secure Data Storage in Cloud Using Cryptographic Algorithms. *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*.
[5] Guo, C., Tian, P. and Choo, K., 2021. Enabling Privacy-Assured Fog-Based Data Aggregation in E-Healthcare Systems. *IEEE Transactions on Industrial Informatics*, 17(3), pp.1948-1957.
[6] Rajeswari, S. and Kalaiselvi, R., 2017. Survey of data and storage security in cloud computing. *2017 IEEE International Conference on Circuits and Systems (ICCS)*
[7] Singh, I., Kumar, D. and Khatri, S., 2019. Improving The Efficiency of E-Healthcare System Based on Cloud. *2019 Amity International Conference on Artificial Intelligence (AICAI)*,
[8] Hameed, R., Mohamad, O., Hamid, O. and Tapus, N., 2015. Design of e-Healthcare management system based on cloud and service oriented architecture. *2015 E-Health and Bioengineering Conference (EHB)*.
[9] Abdul Karim, N. and Ahmad, M., 2010. An overview of electronic health record (EHR) implementation framework and impact on health care organizations in malaysia: A case study. *2010 IEEE International Conference on Management of Innovation & Technology*.
[10] Zhang Jing, Wang Jinsu, Zheng Zhuangfeng and Zhao Chongan, 2016. Cloud storage encryption security analysis. *2016 IEEE International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*.
[11] Wan-Young Chung and Ee May Fong, 2014. Seamless personal health information system in cloud computing. 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society,
[12] Yang, C. and Liu, C., 2013. Developing IHE-Based PHR Cloud Systems. 2013 International Conference on Social Computing.
[13] Mahmood, Z. and Ibrahem, M., 2018. New Fully Homomorphic Encryption Scheme Based on Multistage Partial Homomorphic Encryption Applied in Cloud Computing. *2018 1st Annual International Conference on Information and Sciences (AiCIS)*,.
[14] Veeraragavan, N., Arockiam, L. and Manikandasaran, S., 2017. Enhanced encryption algorithm (EEA) for protecting users' credentials in public cloud. *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*,.
[15] Nivedhaa, R. and Justus, J., 2018. A Secure Erasure Cloud Storage System Using Advanced Encryption Standard Algorithm and Proxy Re-Encryption. *2018 International Conference on Communication and Signal Processing (ICCSP)*,
[16] Masrom, Maslin, and Ailar Rahimli. "A Review of Cloud Computing Technology Solution for Healthcare System." Research Journal of Applied Sciences, Engineering and Technology 8, no. 20 (2014): 2150–2155.
[17] HUCÍKOVÁ, Anežka, and Ankica Babic. "Cloud Computing in Healthcare: A Space of Opportunities and Challenges." Transforming Healthcare with the Internet of Things (2016): 122.
[18] Yang, Haibo, and Mary Tate. "A descriptive literature review and classification of cloud computing research." CAIS 31 (2012): 2.
[19] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation computer systems 28, no. 3 (2012): 583–592.
[20] Nigam, Vaibhav Kamal, and Shubham Bhatia. "Impact of Cloud Computing on Health Care." (2016).
[21] ―How to Improve Healthcare with Cloud Computing‖, By Hitachi Data Systems, white paper, (2012).
[22] Mehraeen, Esmaeil, Marjan Ghazisaeedi, Jebraeil Farzi, and Saghar Mirshekari. "Security Challenges in Healthcare Cloud Computing: A Systematic Review." Global Journal of Health Science 9, no. 3 (2016): 157.
[23] Sun, Dawei, Guiran Chang, Lina Sun, and Xingwei Wang. "Surveying and analyzing security, privacy and trust issues in cloud computing environments." Procedia Engineering 15 (2011): 2852–2856.
[24] Khan, Nabeel, and Adil Al-Yasiri. "Identifying cloud security threats to strengthen cloud computing adoption framework." Procedia Computer Science 94 (2016): 485–490.
[25] Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security issues for cloud computing." Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies 150 (2012).