ASAFE G-CLOUD BASED FRAMEWORK TO IMPROVE GOVERNMENT HEALTHCARE SERVICES

P. Vijay Bhaskar Reddy
Associate Professor, Head of Dept. of Master of Computer Applications,Narayana Engineering College,Gudur.

K. Kaveri
PG Scholar, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur.

Abstract **-** Within the literature, we have witnessed in the healthcare sector, the growing demand for and adoption of software development in the cloud environment to cope with and fulfill current and future demands in healthcare services. In this paper, we propose a flexible, secure, cost effective, and privacy preserved cloud-based framework for the healthcare environment. This framework aims to provide health services and facilities from the government to citizens. Furthermore, multifactor applicant authentication has been identified and proofed in cooperation with two trusted authorities. Security analysis and comparisons with the related frameworks have been conducted.

Keywords: Attribute-based Encryption, Health Record, Ciphertext Policy, Authentication, Authorization.

I.INTRODUCTION

A common phenomenon in healthcare in most Arab countries is the lack of optimal utilization of human and material resources available to provide integrated healthcare to prevent diseases and treat diseases after they occur. Statistics indicate that Arab countries suffer from high rates of health problems, such as diabetes, liver disease, and parasitic diseases, such as histosomiasis and malaria. These health problems could be prevented before they occur or their complications prevented by early detection. This is due to a combination of factors: planning, operational, and technical. If we were able to overcome them, this would lead to significant progress in the level of health care.

In addition, there is a weakness and lack of available hospital information systems, which is some of the most advanced software that directly serves all technical and administrative healthcare activities, ensuring that the medical institution has full control over all its activities and resources. The successes of these advanced systems do not depend on the exact selection of equipment and software for storage. Rather, their success depends on their suitability for different users—from healthcare providers, such as doctors, nurses, technicians, and even administrators—where the vision and priorities of each of these categories differ, and their information needs vary, as do the benefits of each of these systems.

The traditional health system (paper) has been replaced by an electronic health information system because the traditional system has been found to be ineffective due to a number of issues, including low storage capacity, high operating and maintenance costs, and system integration [1]. The computerized health system was then replaced by cloud computing because it relies on a more efficient infrastructure, as well as the many benefits of cloud computing in IT, such as cost, scalability, flexibility, and other features [2]. The use of cloud computing in electronic health records reduces costs in the provision of health services, maintenance costs, networks, licensing fees, and infrastructure in general, and this will therefore encourage developers to adopt the cloud in healthcare [2], [3].

The rapid shift to the cloud and its use in healthcare systems has raised concerns about crucial issues of privacy and information security [4], [5]. The adoption of the cloud in IT increases the focus and concern of healthcare providers on clinical and patient-related services and reduces attention on infrastructure management [6]. The sharing of personal and health information across the Internet and various servers outside the safe environment of the healthcare institution has led to a number of problems related to privacy, security, access, and compliance issues [7], [8], [9], [10].

II. BACKGROUND WORK

This section review the needed background for any proposed design based on CP-ABE for a cloud based EHR systems.

A**. Elliptic Curve Cryptography:** Elliptical curve cryptography (ECC) is a type of PublicKey cryptosystem based on of elliptic curve theory. ECC security relies on elliptic curve logarithm problem. Elliptic curves groups for cryptography are examined with the underlying fields of Fp (where p>3 is a prime) and F2m (a binary representation with 2m elements) [12]. ECC can be used in conjunction with most public key encryption methods, such as RSA, El Gamal, and Diffie-Hellman. ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower processing power, it is becoming widely used on compact platforms such as mobile applications and smart cards.

B. **Bilinear Pairing**: Bilinear mapping is used to construct a relationship between two or more groups with efficient pairing operation

C. Cloud-Based EHR Schemes: In this section, we review the most important algorithms that contributed to the development of cloud-based healthcare. In 2006, Goyal et al. [11] proposed a new idea in encryption called attribute-based encryption (ABE). In the ABE scheme, ciphertexts and users' secret keys are associated with a set of attributes. A user can decrypt a ciphertext if, and only if, there is a match between its secret key and the ciphertext. ABE has been applied and tested in many cloud-based applications.

III.PROPOSED WORK

We propose a secure and efficient framework for the government EHR system, in which fine-grained access control can be afforded based on multi-authority cipher text attribute-based encryption (CP-ABE), together with a hierarchical structure, to enforce access control policies.

The framework uses cloud computing to develop health services provided by the Ministry of Health to citizens. This framework aims to provide health services and facilities from the government to citizens (G2C).It provides a flexible,secure,and cost-effective and privacy preserved G-cloud-based framework for government healthcare services.

System Model: The system model consists of the following modules, shown inFigure-1.

HCSP: In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the patient's details and will do the following operations like Upload Patient Details, View All My Uploaded Patients, View Public Keys, and View Transaction Details.

Patients:In this module, user logs in by using his/her user name and password. After Login user requests search control to cloud and will Search for Patients 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.

E-Govt 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 name and password. After Login he will do some operations like View all Patients, Generate Public Key Requests, Key Generation.

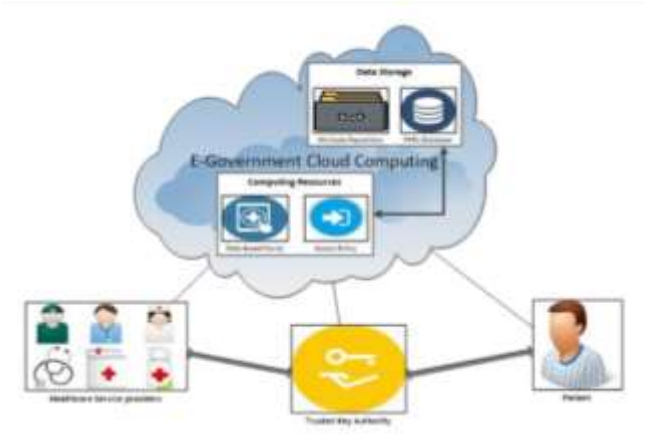

Fig.1: G-Cloud-Based Framework

The e-Government cloud-based EHR consists of the following cloud services:

The first service consists of two fundamental parts: data repository and computing resources. The first service is responsible for storing the encrypted EHRs that are accessible only by the authenticated healthcare providers through an access policy based on healthcare provider attributes. The second service is responsible for generating the access policies, providing efficient keys management, and performing other required computing processes. The third service is hosting the web-based portal. The developed web-based portal should be a secure online website that can be accessed by the stockholders from anywhere, with 24-hour a day access, through Internet connection, and can be accessed by any device.

IV. ANALYSIS OF FRAMEWORK

A) Security Analysis: The proposed hierarchical multi-attribute authority CPABE framework in the EHR cloud environment satisfies the following security requirements:

Data Privacy: The proposed framework protects users' privacy. The EHR's privacy is satisfied when the user uploads the message encrypted with the access policy privileges settled by the user's own policy and is protected by authority attribute domains.

Fine-grained access control: The proposed framework is designed in a way that after successful identity authentication, different applicants will have different access privileges according to the attribute key generator and the access policy used by the user.

Efficiency: The computational overhead completed by the government or the central authority can be reduced greatly by assigning tasks to the attribute domain authorities. The proposed scheme enforces attribute domain authorities to generate and distribute keys to the entities. In general, applying multiple attribute domain authorities can efficiently distribute the computational overhead over multiple domain authorities because each authority will be not overloaded.

Scalability: Migrating and adopting the patients' records from the inhouse servers existing in any healthcare centers to the cloud has many advantages in comparison with traditional client servers systems. Scalability is one advantage of such migration. The cloud-based EHR system requires less ITresources, reducing operating costs, improving accessibility and collaboration, ensuring simpler implementation, delivering new services, and ensuring better scalability. Our proposed scheme improves the scalability of the system but limits the impressibility of the access policy because it only supports conjunctive policy across multiple AAs.

B)Performance Analysis: Standard coding techniques that rely on the use of keys in encryption and decryption are not well suited for use in cloud-based applications, especially those related to healthcare systems.

Symmetric-key encryption: These techniques are effective in many applications but are more complicated in healthcare applications as they require additional mechanisms to implement access control. This is especially true when healthcare providers all use a shared key to encrypt and decrypt, so if this shared key is hacked, the whole healthcare system will be compromised.

Public-key encryption: These techniques are not considered to be practical because they require an expensive infrastructure for the public key to maintain the distribution and management of public keys.

V. CONCLUSION

In this paper, we proposed a secure cloud-based EHR framework that guarantees the security and privacy of medical data stored in the cloud, relying on hierarchical multi-authority CP-ABE to enforce access control policies. The proposed framework provides a high level of integration, interoperability, and sharing of EHRs among healthcare providers, patients, and practitioners. The proposed scheme can be adopted by any government that has a cloud computing infrastructure and provides treatment services to the majority of citizen patients. Future work includes implementing and evaluating the proposed scheme in a real-world environment.

REFERENCES

1. Masrom, Maslin, and AilarRahimli. "A Review of Cloud Computing Technology Solution for Healthcare System." Research Journal of Applied Sciences, Engineering and Technology 8, no. 20 (2014): 2150–2155.
2. HUCÍKOVÁ, Anežka, and AnkicaBabic. "Cloud Computing in Healthcare: A Space of Opportunities and Challenges." Transforming Healthcare with the Internet of Things (2016): 122.
3. Yang, Haibo, and Mary Tate. "A descriptive literature review and classification of cloud computing research." CAIS 31 (2012): 2.
4. Zissis, Dimitrios, and DimitriosLekkas. "Addressing cloud computing security issues." Future Generation computer systems 28, no. 3 (2012): 583–592.
5. Nigam, Vaibhav Kamal, and Shubham Bhatia. "Impact of Cloud Computing on Health Care." (2016).
6. How to Improve Healthcare with Cloud Computing‖, By Hitachi Data Systems, white paper, (2012).
7. Mehraeen, Esmaeil, MarjanGhazisaeedi, JebraeilFarzi, and SagharMirshekari. "Security Challenges in Healthcare Cloud Computing: A Systematic Review." Global Journal of Health Science 9, no. 3 (2016): 157.
8. 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.
9. Khan, Nabeel, and Adil Al-Yasiri. "Identifying cloud security threats to strengthen cloud computing adoption framework."Procedia Computer Science 94 (2016): 485–490.
10. Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and BhavaniThuraisingham. "Security issues for cloud computing." Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies 150 (2012).
11. Goyal, Vipul, OmkantPandey, AmitSahai, and Brent Waters. "Attribute-based encryption for fine-grained access control of encrypted data."In Proceedings of the 13th ACM conference on Computer and communications security, pp. 89–98.Acm, 2006.
12. Hankerson, Darrel, and Alfred Menezes. Elliptic curve cryptography.Springer US, 2011.

Author's Profile:

P. Vijay BhaskarReddyhas received his PG degree in Master of Computer Applications from Geethanjali Institute of PG Studies, affiliated to S V University, Tirupathi in 2008 and M. Tech. degree in Computer Science from

Gokula Krishna College of Engineering, affiliated to JNTU, Anantapur. At present he is the Head of the Dept. of MCA &Associate Professor in Narayana Engineering College, Gudur, AndhraPradesh, India.

K. Kaveri has received her B.Sc Degree in Computer Science fromViswamDegree College Nayudupeta, affiliated to VikramaSimhapuri University, Nellore in 2017 and pursuing PG Degree in Master of Computer Applications (M.C.A) from Narayana Engineering College, Gudur affiliated to JNTU Anantapur, Andhra Pradesh, India.