A Secure G Cloud Based Framework for Government Healthcare Services

[1]Prof.Kanchan Umavane, [2]Mr. Sachin Alam, [3]Mr. Manish Bhoir, [4]Mr. Aniket Dhasade
[1]Asst.Professor,[2,3,4]UG Student,[1,2,3,4]Computer Engg. Dept. Shivajirao S. Jondhle College of Engineering & Technology, Asangaon, Maharashtra, India.
[1]kanchanumavane2020@gmail.com, [2]sachinalam4216@gmail.com, [3]manishbhoir259@gmail.com, [4]aniketdhasade77@gmail.com

Abstract - The healthcare industry witnesses a rising need for and acceptance of cloud-based software development to address and meet the present and forthcoming requirements in healthcare provision. This initiative presents attributes including a versatile, safeguarded, cost-efficient, and privacy-conscious cloud-based framework tailored for healthcare settings. It introduces a resilient and efficient framework for the government's Electronic Health Record (EHR) system. This framework incorporates sophisticated access control mechanisms facilitated by multi-authority ciphertext attribute-based encryption (CP-ABE), alongside a hierarchical structure. The suggested platform enables global influence-makers to enhance the medical services industry and leverage the current e-government cloud computing infrastructure. The conventional framework is tasked with providing shared services within a highly efficient, dependable, and secure setting. Its primary objective is to deliver government health services and amenities to citizens (G2C). [1]

Keywords – Attribute Based Encryption, Cloud Computing, Artificial Network, Data Management

I. INTRODUCTION

The Electronic Health Record system is also decentralized system which have cloud applications in medical field, it replaced the traditional health system because the traditional health system was inefficient due to several factors such as low storage capacity, higher operating and maintenance costs and system integration issues. The computerized health system transitioned to the cloud due to its superior infrastructure and the multitude of advantages it offers in IT, including cost-effectiveness, scalability, and various other features. The implementation of cloud computing in electronic medical records leads to a reduction in expenses associated with delivering health services, maintaining systems, managing networks, and acquiring licenses and infrastructure. The cloud's use in healthcare IT increases the focus and interest of healthcare providers in clinical and patient-centric services management. The act of sharing personal and health data over the internet and across servers external to the secure confines of healthcare institutions has brought forth numerous concerns regarding privacy, security, access, and compliance.[1]

To address the difficulty of knowledge access control in cloud storage, there are quite few schemes proposed, among which Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is considered one among the foremost promising techniques. A salient feature of CPABE is that it grants data owners direct control power supported access policies, to supply flexible, fine grained and secure access control for cloud storage systems.[10]

II. AIMS AND OBJECTIVE

a) Aim

The aim of this system is to create a secure and effective framework for the Government Health Information System (HERS) that provides fine-grain access control using multi-author authority cipher text (Cipher-ABE) attribute-based encryption, as well as a hierarchical structure to enforce access control policies. The aim of this framework is to deliver government health services and facilities to citizens (G2Cs). Multifactor applicant authentication (MFA) has been recognized and verified through collaboration with two reputable entities. Security analysis and comparisons with related frameworks have also been conducted. [1]

b) Objective

Main objective is to create a decentralized system, a totally transparent and hospitable database, which brings transparency to the patient and the governance data and removes the satiation of central servers and provides interaction among counterparts [1].

It basically contains 4 objectives.

1.Cloud Based: All the data which is stored need to be in cloud-based storage model.

2. Security: Attribute Based Encryption is used for securing both client and server key access.

 DOI : 10.35291/2454-9150.2024.0258

3. Healthcare Service Provider: It takes care of everyone networks and data in cloud storage server also gets ciphered and only approved users can decipher the data.

4. Input Design: Entering data using screens allows users to receive helpful messages as needed, preventing confusion, and ensuring a user-friendly input design layout.

Thus, objective is to create an input layout that is easy to follow. Above are the core objectives of this system which needs to be fulfilled.

III. LITERATURE SURVEY

Paper 1: A Review on Cloud Computing in Healthcare Sectors

Cloud computing emerges as a novel technology providing software infrastructure and computational platforms as services accessible over the Internet from anywhere at any time. Advocates suggest that cloud computing holds promise in resolving numerous challenges encountered within the healthcare system, including expanding storage capacities, and enhancing existing capabilities.

Hence, the aim of this study is to investigate the potential of cloud computing can be present as a solution to address various issues within healthcare information systems. Notably, the study delves into challenges such as data transmission, storage, as well as cost and maintenance concerns, offering detailed descriptions and analysis [2].

Paper 2: Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption:

This paper proposes the unique ABE-based paradigm for patient-centric secure PHR sharing in multi owner cloud computing systems is proposed in this study. To tackle the primary managerial obstacles, it divides system users conceptually into two groups. Domain kinds, specifically public and private domains (PSDs).

Specifically, in the previous system, attribute authorities managed the bulk of professional users in a distributive manner, and each owner only had to handle a limited number of users' keys within their personal domain. Additionally, Use of ABE which can be access only by authorized users.[7]

Paper 3: An Enterprise Cloud-Based Electronic Health Records System:

An Enterprise Cloud-Based Electronic Health Records System: Because of the high upfront costs and ongoing maintenance associated with EHRs, their adoption in healthcare facilities has been sluggish despite their potential to alleviate the issues and constraints of the paper-based method. Cloud computing is widely acknowledged as the computer infrastructure of the next generation, providing numerous benefits to its users. An Enterprise Electronic Cloud-Based Health Record System for patient data collection, retrieval, archiving, and updating was created, put into use, and tested for this system.[6]

IV. EXISTING SYSTEM

Existing System is based on the infrastructure which required patient to physically attend. Health issues can potentially be averted through preventive measures, or their complications mitigated through early detection. This outcome results from a convergence of planning, operational, and technical considerations. Overcoming these challenges would undoubtedly result in notable advancements in healthcare delivery.[1]

V. COMPARATIVE STUDY

Sr. No.	Author	Paper Title	Publication	Technology	Purpose
1.	Sanaa Sharaf, and Nidal F. Shilbayeh	A Secure G Cloud Based Framework for Government Healthcare Services	IEEE,2019	Cloud Computing	Proposes framework for Electronic Healthcare Records
2	Ebtisam Ali Abdullah and Anwar Saif Alshamiri	A Review on Cloud Computing in Healthcare Sectors	IRJMETS, 2020	Cloud Computing	Use of Concept Called “E-Health Cloud”
3	Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou	Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption Images	IEEE,2013	Cloud Computing	Introduces Electronic Health Record concept.
4.	Adebayo A. Abayomi-Alli, Aderonke J. Ikuomola, Ifeoluwa S. Robert and Olusola O. Abayomi-Alli	An Enterprise Cloud-Based Electronic Health Records System	Journal of Computer Science and Engineering Technology,2014	Cloud Computing	An architecture for segmenting and classifying brain tumors using three tumor types.

VI. PROBLEM STATEMENT

The problem with the ABE-based encryption scheme is that data encryption needs to use the public key for each licensed user and needs to use attributes to control the user's access to the system. Also, ABE based encryption scheme offers no scalability and has an average efficiency with no support for multiple authentication which is available in the proposed system. [1]

VII. PROPOSED SYSTEM

 DOI : 10.35291/2454-9150.2024.0258

The proposed framework is based on Cipher Text Policy Attribute Based Encryption (CP-ABE) which is more secure and more efficient in comparison with other existing frameworks. To accomplish fine-grained access control, it makes use of numerous authority attribute domains that apply varying access privileges for certain applicant categories.

This implies that in order to access the necessary data, every attribute needs to meet the user access policy structure. It is governed by a trustworthy government entity and employs multi-factor authentication. The suggested plan benefits from the government-provided infrastructure and facilities and is appropriate for G-based cloud EHR systems. [1]

VIII. ALGORITHM

Step 1: Setup

This algorithm receives a security parameter, denoted as K, as input, and produces the primary key (PK) and the master key (MK) as outputs.

Step 2: Create Attribute Authority (AA, PK)

The verified authority is responsible for executing this algorithm with AA as input. Generating identification for attribute authority, with attributes as Sid, Sk Aid

Step 3: Attribute Key Generator (PK, SKAid, Sid)

```
public static void main(String[] args) {
AccessKeyGenerations gsk = new AccessKeyGenerations();
char spacerChar = 'D';
String key = gsk.randomUUID(15, 0, spacerChar);
System.out.println("Key "+key+" And its Length is "+key.length());
}
```

In this stage the primary key and domain entity and other attributes are taken as inputs to produce secret keys.

Step 4: Encrypt (PKU, PK, P)

In this stage the encryption algorithm receives message M, primary key PK and entry policy (EP), and common users (CU) as inputs and generates cipher-based messages (CT).

Step 5: Decrypt (CU, EP, CT, PK, M)

```
Session session = Session.getDefaultInstance(props,
 new javax.mail.Authenticator() {
 protected PasswordTextAuthentication
getPasswordTextAuthentication() {
 return new
```

The decryption algorithm requires the primary key (PK), a ciphertext message (CT), the same access policy (P) used during encryption, the secret user key (SKUj), and the set of secret attribute keys (SKA) as input.

XI. MATHEMATICAL MODEL

Elliptic Curve Cryptography:

Elliptic Curves: Consider FP as a finite field with a prime number p > 3. The elliptic curve y^2 = x^3 + ax + b over Zp consists of solutions (x, y) ∈ Zp x Zp satisfying the congruence:

• y^2 ≡ x^3 + ax + b (mod p) Here, constants a ∈ Zp and b ∈ Zp are such that 4a^3 + 27b^2 ≠ 0 (mod p). Additionally, the curve includes a unique point O known as the infinity point.

• If E represents an elliptic curve over a field F, the elliptic curve discrete logarithm to base Q ∈ E(F) entails finding an integer n ∈ Z such that P = nQ for a given point P ∈ E(F). [1]

Attribute Based Encryption:

Here's a simplified protocol implementing the functionality over a prime-order group, based on the Diffie-Hellman assumption:

Step 1) Party A (Authority) masks each h by randomly sampling r ∈ Zp, setting a_i = (h, g^r), and sends each a_i to party U.

Step 2) Party U (User) then samples t_i < Zp and computes b_i = (h)^t_i * (g^r)^t_i for each i, sending them back to A.

Step 3) Finally, A computes c_i = ∏(b_i) and sends the value to U, who computes the desired value as c = ∏(b_i) * g^t.

In this protocol:

- g is a generator of the group.
- h, a_i, and b_i are elements of the group.
- r and t_i are randomly sampled from Zp denotes the group operation.
- ∏ denotes the product of all elements.

X. SYSTEM ARCHITECTURE

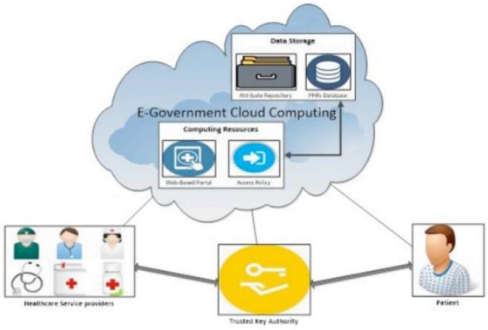

Fig.1: System Architecture

Description:

It represents proposed secure cloud-based framework architecture for government healthcare services, including

 DOI : 10.35291/2454-9150.2024.0258

cloud computing, Health service provider, Cloud Storage and file owner. The system consists of the operating system, a fully functional application and a signal function unit. It has a flat design, and all applications are based on the cloud platform, which are called "user". Health Service Provider is the mediation layer used for communication. It can process and store metadata uploaded by the owner. On the user side, any cryptographic algorithm, like the Elliptic cryptographic algorithm, like the Elliptic Curve Digital Signature Algorithm, is used to confirm the identity of the data owner quickly Users (cloud side) can provide online storage services, having received an upload request from the owner (user side). The cloud storage facility can verify the owner's permission through the authentication unit, the upload unit, the file storage unit and the mapper. [1].

XI. ADVANTAGES

- Cloud-based storage systems are a great way to store EMRs because they are accessed from any device at any time.
- Clinical and patient-related services are prioritized, thereby reducing focus on infrastructure management.
- One crucial advantage is enhanced security. Each system operates autonomously and is overseen by a central trusted authority.
- In less quantity of data, it can achieve more accuracy.

X. DESIGN DETAILS

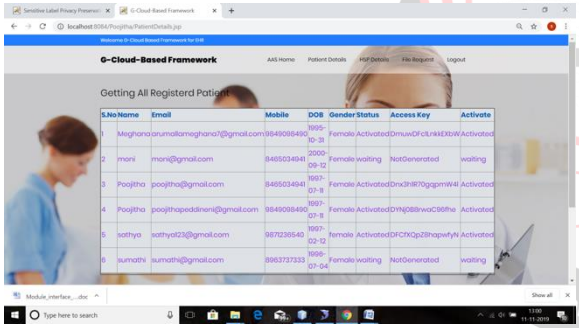

Fig 1: Patients Data

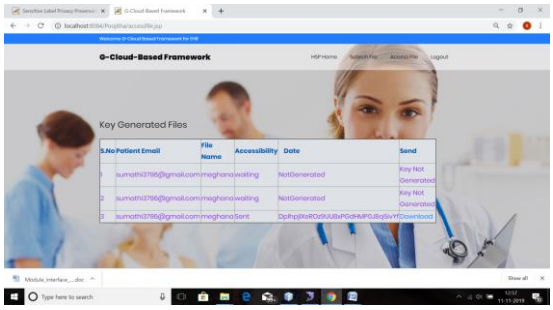

Fig 2: HSP Key Generation

XI. CONCLUSION

Thus, we have tried to implement the paper of Authors: Sanaa Sharaf, and Nidal F. Shilbayeh, "A Secure G Cloud based Framework for Government Health Care Services", IEEE 2019 and according to the implementation, this work develops a Secure G Cloud-based platform for government health care services which makes two main contributions: An anonymous patient report file sharing mechanism which provides privacy, data sharing. A mechanism for inspecting files identifying illegal uploads. These both are combined, and file sharing is performed to achieve real power dispersion and data sharing. Creates a platform where Health service providers can access patient data directly with help of public key encryption technique.

REFERENCE

[1] Sanaa Sharaf, and Nidal F. Shilbayeh "A Secure G Cloud Based Framework for Government Healthcare Services" IEEE Access, 2019.

[2] Ebtisam Ali Abdullah and Anwar Saif Alshamiri "A Review on Cloud Computing in Healthcare Sectors" International Research Journal of Modernization in Engineering Technology and Science Volume 02/Issue:08/August - 2020

[3] 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 (July - 2016): 157

[4] Nigam, Vaibhav Kamal, and Shubham Bhatia. "Impact of Cloud Computing on Health Care." International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 05 | May – 2016

[5] Khan, Nabeel, and Adil Al-Yasiri. "Identifying cloud security threats to strengthen cloud computing adoption framework." Procedia Computer Science 94 (2016): 485–490.

[6] Adebayo A. Abayomi-Alli, Aderonke J. Ikuomola, Ifeoluwa S. Robert and Olusola O. Abayomi-Alli "An Enterprise Cloud-Based Electronic Health Records System", Journal of Computer Science and Information Technology June 2014, Vol. 2, No. 2, pp. 21-36

[7] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE Transactions on Parallel And Distributed Systems, Vol. 24, No. 1, January 2013

[8] Yang, Haibo, and Mary Tate. "A descriptive literature review and classification of cloud computing research." CAIS 31 (2012): 2.

[9] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation computer systems 28, no. 3 (2010): 583–592.

[10] Prof. Swapnil Wani, Mr. Javed khan, Miss.Anamika Jaiswar, Miss.Priyanka Gujar "RAAC With Multiple Attribute Authority For Public Cloud", International Journal for Research in Engineering Application & Management, Vol-06, Special Issue, June 2020.

 DOI : 10.35291/2454-9150.2024.0258