A Data Integrity and Security Approach for Health Care Data in Cloud Environment

A. Sonya[1] and G. Kavitha[2*]

[1]Department of Information Technology, B.S. Abdur Rahman Crescent Institute of Science and Technology, India. sonya@crescent.education

[2*]Department of Information Technology, B.S. Abdur Rahman Crescent Institute of Science and Technology, India. gkavitha.78@crescent.education

Received: August 22, 2022; Accepted: October 16, 2022; Published: November 30, 2022

Abstract

Healthcare digitalization has turned out to be a significant paradigm in the advancement of medical sector. Resultant, there is production of huge volume of patient's digital information. Moreover, storing and safeguarding such information tends to become a critical point of concern. The cloud technology assures to be an effective mechanism towards handling and distributing healthcare information by attending the concerns pertaining to data integrity, security and privacy. The significant benefits and accessibility offered by the cloud technology has immensely raised the storage of healthcare information. It's highly important that the sensitive healthcare data residing in the cloud is completely secured amidst the healthcare providers and the cloud server. There has been a rising concern associated with secured data access within the cloud environment. That is, the cloud framework must assure a robust authentication control mechanism which allows the healthcare users to confidently share medical information across it. Towards accomplishing the same, a secured and light weight data access management system has been recommended that promises data Integrity and Security. Moreover, the proposed system offers the feature of authority control authorization and authentication mechanism for safeguarding the health-related data residing and circulating within the cloud. A CIAM (Customer identity and access management) helps in secured Data Access Control and OAuth 2.0 aids in providing right privilege with authorisation. Also, by the means of Progressive Attribute Based Encryption approach, sensitive medical information can be encrypted from the cloud storage in a secure manner. The proposed light weight framework yields in efficient, reliable and stable output within the cloud.

Keywords: Security, Cloud Environment, Authentication, Authorization, Data Integrity, CIAM, OAuth 2.0.

1 Introduction

Apparently, Cloud storage signifies the core component when considering the cloud computing technology as per [1]. It primarily enables the users to host their sensitive over the cloud. Though the data hosting approach is highly beneficial but simultaneously it confronts the issue pertaining to the data access control according to [2]. Possibly, the cloud server may grant access to the unauthorized

Journal of Internet Services and Information Security (JISIS), volume: 12, number: 4 (November), pp. 246-256
DOI: *10.58346/JISIS.2022.I4.018*

*Corresponding author: Department of Information Technology, B.S. Abdur Rahman Crescent Institute of Science and Technology, India.

users either for monetary gain or due to lack of robust data access controls, thus compromising on the trust and reliability of numerous cloud users as mentioned by [3]. The proposed system integrates with the cloud in order to ensure user-based authentication and authorization so as to strengthen the data access control mechanism and safeguard the healthcare data and resources as put forth by [4]. In brief, the electronic medical record represents information pertaining to an individual's health, comprising of examination, lab tests, allergies, medication history, and claims. In addition, the patient's health record may also comprise of: physician requirement of fetching patient's record [5]. As per the norms, the medical firm ensures that there is integrity and privacy of the patient's medical records and so the patient is asked to sign a consent form that clearly denotes with whom the patient want to share its private data. Albeit, such paper-based consent need not imply to all the patients as specified by [6] and neither they may be able to put forth their requirements specifically. Moreover, there is no provision of communicating such paper-based consent and the access control policies associated with it either electronically or automatically among the enterprises, mentions [7]. By the means of user-centric authentication and authorization, a unique identifier is allocated to the individual for logging to the desired service. The user can also state access control policies for regulating its data/resources present in the cloud to be accessed by various health services as indicated by [8]. The related work pertaining to the cloud security, authentication, and authorization. The solution section briefs regarding an approach for securely accessing the applications in the cloud storage. The result and discussion section presents the system's overall performance along with the output generated. Eventually, the crux or the conclusion of the proposed work is laid down in the Conclusion section.

2 Related Work

There have been multiple approaches and methodologies suggested for dealing with the concerns pertaining to the authentication and access control within the cloud as indicated by [9]. The prevailing encryption model comprises of a group of essential attributes that are linked with each data file. A public key is associated with each attribute for enforcing access policies as put forth by [10]. These public key enables encryption of data files. Depending on the secret keys, an access structure is framed for the users, as per [11]. The user can decrypt a cipher text (based upon its access structure) during file access. All the data files must be re-encrypted by the data owner that is accessible to a revoked user, states [12]. And for doing so, a combination of Elliptic Curve Cryptography (ECC) with proxy re-encryption has been utilized, indicates [13,14]. The above approach pays no attention to the handling of data access policies. [15,16] Put forth a patient-centric and fine-grained data access control by the means of a multiple-owner setting framework. Resultant, the data encryption can be performed by numerous patients (rather data owners) with the help of the different cryptographic keys. Moreover, they have the provision to define the access structure of various users by data encryption based on certain attribute set. There is recommendation of a combination of two or more security policy for WBANs (wireless body area networks) by [17] that ensures a protective e-Health care system. It employs the cryptographic techniques namely, two key cryptography such as public key and private key to accomplish session key management and data encryption respectively in WBANs as per [18]. A hierarchical identity-based encryption has been proposed by [19] for user classification into upper and lower levels. The upper-level users have the provision to share the cloud storage services with the lower-level users. There can be multiple lower-level users (recipients) that can be listed by the upper-level user (senders) by considering the recipients number and public keys which acts as an input for the hierarchical identity-based encryption algorithm. It's strictly ensured by the algorithm that the upper-level users or the recipients only can decrypt the file through their private keys as put forth by [20].

3 Description of Proposed Framework

Herein lies the description of the system and security model with respect to the approach of authority access control for cloud storage.

3.1. System Architecture

The basic system diagram of cloud storage framework which basically comprises of an Authentication, Authorisation mechanism built primarily for the system access control. Also, there is utilization of secured communication via progressive Attribute Based Encryption techniques for constructing the cloud storage framework. This works appropriately for confidential and secure medical data outsourced by the data owner to the cloud storage and also for fetching the sensitive data knowledge by the data consumer. Before carrying out any data access related activity, it's mandatory that the user is registered in CIAM (Customer identity and access management) which being an authentication server as shown in figure 1.

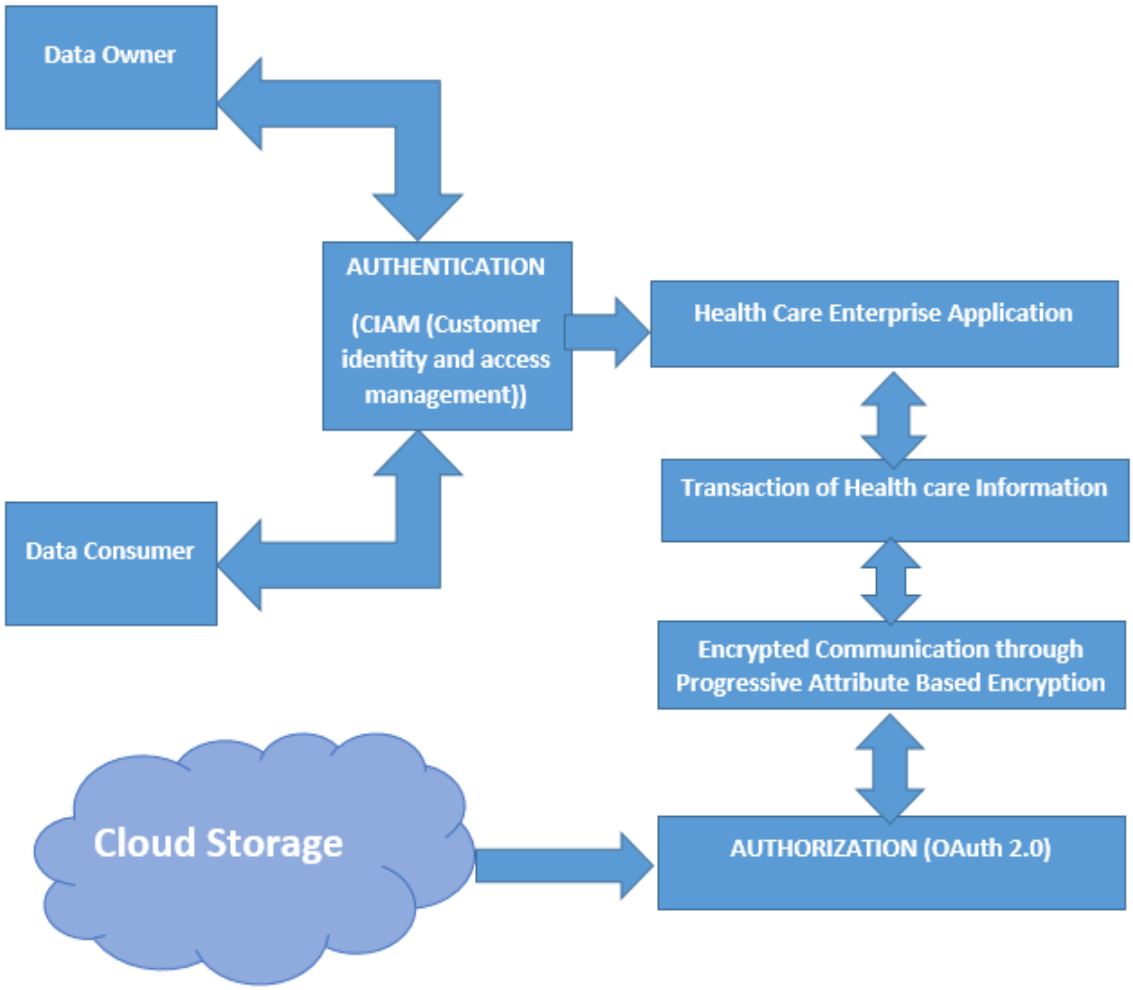

Figure 1: Overall Proposed Architecture

The CIAM holds the client's credentials such as its username and password etc. Only the registered users can login and access the data. Before storing the user's details like username and pass code in the cloud, they are first encrypted. There is thorough analysis of the results generated from the proposed

new model with respect to the security parameters in cloud computing. As soon as any user puts a request for accessing records from Health Care Enterprise Application, the proposed system comes into action. It prompts the user for an Access Control mechanism and authenticates it via CIAM (Customer identity and access management). The authorized or registered user is then allowed to access the data. Thereafter, an authorisation mechanism via OAuth 2.0 is enforced to the 'data access grant request that enables accessing the cloud services. Thereafter, there is secure transfer of the requested information via progressive Attribute Based Encryption mechanism that is responsible for encrypting the sensitive medical information within the cloud using secured communication.

3.2. Authentication CIAM in Health Care Application

Implementation of effective and robust Customer Identity and Access Management (CIAM) ensures security of eHealth enterprises and prevents the concern related to data breaches. Also CIAM capabilities aids in authorizing patient information thus supporting data protection regulations. The paradigm of customer identity access management is an effective solution in building the platform amidst the data customers and the eHealth enterprise applications thereby ensuring safety of identity and personal information. The CIAM involves various processes and it begins with the registration of the user. Only the registered and authorized users are permitted to access or view the relevant patient's information. The overall CIAM process flow along with the internal architecture is depicted in Figure 2. It's made sure that there is a simple registration process comprising of essential credentials of the customer. There is provision of registering with multiple registration options viz. self-registration, social registration or as a delegated administration (say a delegate registering on the user's behalf). But it's also ascertained that the user's identity is verified and approved prior to registering and creating their account. Such a check ensures that the valid user is performing the registration.

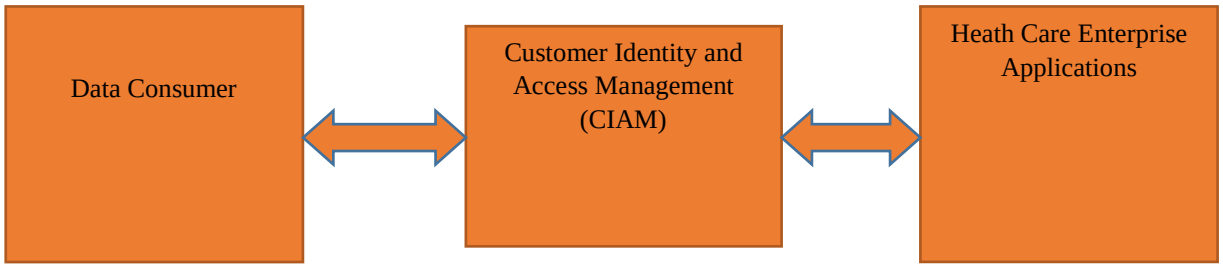

Figure 2: Authentication CIAM Overall Flow

3.3. Authorisation OAuth 2.0 in Health Care Application

One of the open standards for performing authorization is OAuth 2.0 that lays down precise authorization flows along with the authorization decisions, spanning across the web, desktop, and mobile applications. OAuth 2.0 authorization server allocates a secure delegated access token to the client applications (such as Health Care Enterprise Application) using which the client can access resources, be it patients or medical records. Heath Care Enterprise Applications which act as the resource owner decides upon authorizing and granting access to the data consumer. The resource server is responsible for hosting the protected user accounts whereas the user's identity is validated by the authorization server, based on which the user is allocated the access tokens to the application.

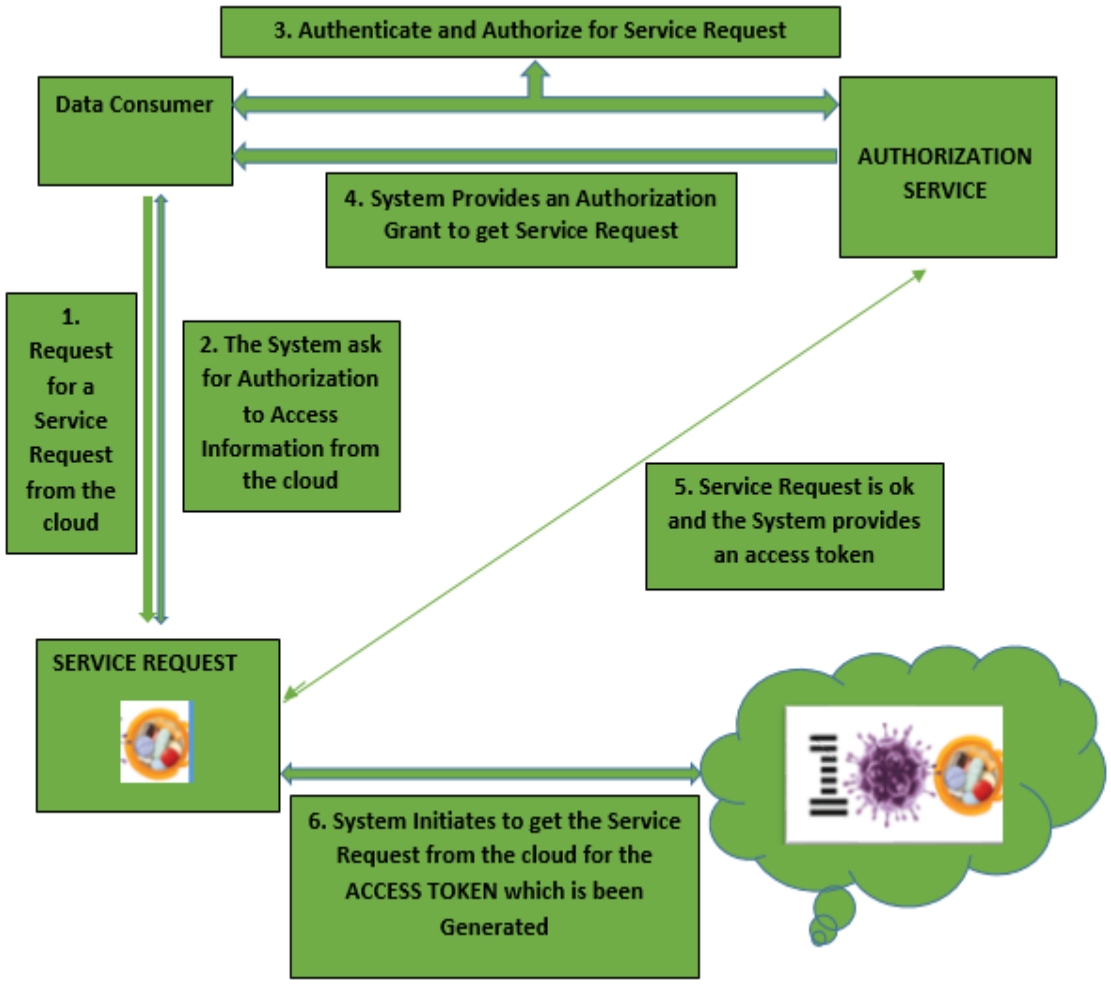

Figure 3: Authorisation OAuth 2.0 Internal Architecture

Tokens are the core component in the OAuth 2.0 standard. To begin, the data consumer is required to input its username and password when prompted by the resource owner. These credentials are then accepted by the authorization server and are validated. If authenticated, the consumer is assigned an access token, using which the data consumer is allowed to access the protected resources residing in the cloud storage. Also, the cloud storage resources are securely shared with the authorized data consumer.

OAuth 2.0 Authorisation Algorithm

Input: Data consumer credentials

Output: Authorisation

Step 1: if Authorisation (Data consumer credentials) == VALID then

Step 2: Access rights = Requesting Access (Token Generation)

Step 3: If Tokens== VALID then

Step 4: Grand = Request based Resource Sharing

Step 5: Breaks the condition

Step 6: else

Step 7: Error condition = Provide Error (rejected message)

Step 8: Grand Access = =Invalid User (unauthorized user)

Step 9: Terminate the process

3.4. Progressive Attribute Based Encryption with Data Integrity

The reformed or updated version of ABE (Attribute Based Encryption) is the PABE (Progressive Attribute Based Encryption) algorithm. PABE represents a public key encryption algorithm, wherein the user's secret key and the cipher text are the primarily attributes. It effectively helps in transferring the sensitive medical data residing in the cloud storage to the authorized data consumer in a secure manner. Both encryption and decryption are performed by PABE with respect to the user attributes and an access structure. The health care environment makes use of certain attributes for building an access structure so that the data consumers can access the medical information residing in the cloud.

Algorithm: Progressive Attribute Based Encryption

Input: Encrypts message with output cipher text.

Output: Decrypts cipher text output Original message.

Step 1: The medical descriptive attributes are taken to encrypt data

u_at ← parse_arguments ().

Step 2: Attributes of the form with a value of **PK** are referred to as Public keys and MK Secret Key Access policies.

pk ← deserialize (reading_file (EOF)(p_file))

mk← deserialize(read_file(m_file))

keys← init_prv_params(pk)

Step 3: Dividing the descriptive Attributes message **A** into shares**.**

Step 4: To interpolate, **mk** points are taken and each attribute are taken with a key value pair.

Applying **foreach** user_attrs[i] ∈ {mk⋯mki} **do the process Step 5**

pk buffer ← serialize(pk)

Write to pkbuffer prv_file

Output prv_file

end

Step 6: Encrypted and shares the secrete message **M**.

S**tep 7:** Cipher text CT containing an access policy A with public key K.

S**tep 8:** Set S of attributes, are fed into the decryption process.

S**tep 9:** If the set S of attributes matches the access structure mk.

Step 10: The algorithm decrypts the cipher text and returns original message M.

4 Results & Discussion

For result generation, an Authentication, authorisation and a PABE (Progressive Attribute Based Encryption) algorithm is employed. It introduces a novel method of authentication, authorisation and encrypted access control. The encryption involves defining the users' public keys using a set of attributes and a policy being defined by the party encrypting data over these attributes which decides upon the users who can decrypt. Table 1 and Figure 4 illustrate the overall performance of PABE (Progressive Attribute Based Encryption) along with different operations and duration of processing time.

Table 1: Progressive Attribute Based Encryption Overall Performance

S. No	**Various Operation**	**Approximate Time Taken** (per attribute)
1.	Key Generation	35 ms
2.	Encryption	27 ms
3.	Decryption	0.8 ms

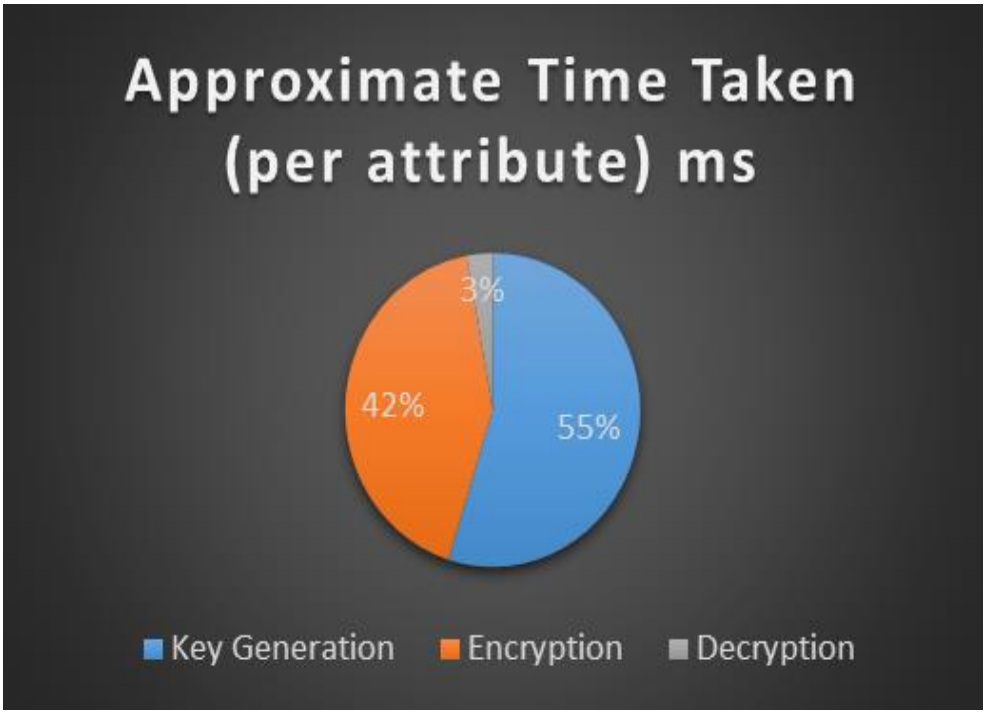

Figure 4: Performance Analysis of Progressive Attribute Based Encryption

It's proved and evident that the encryption execution performed by the above scheme consumes limited time and there is slight increase in the time if number of attributes increase. In contrast to the cryptosystem that relies upon bilinear pairing of ECC, the proposed encryption system stands significantly effective. Moreover, the encryption time is exactly linear with respect to the number of leaf nodes in the access policy, though it's a bit slow. The reason behind this being that the polynomial operations on the tree results into small number of multiplications without affecting the execution time. The results obtained clearly elucidates that the proposed scheme can be practically imbibed for the largest machine instances too. Table 2 and figure 5 illustrate the same.

Table 2: Encryption Time Observation Depending on the Number of Attributes

S. No	Algorithm	Group Size (mb)	Time of Encryption (ms)	Time of Execution (ms)
1	ABE	4.189	3.88	4.36
2	AES	4.189	4.57	4.24
3	RSA	4.367	4.78	3.45
4	PABE	6.337	3.34	3.01

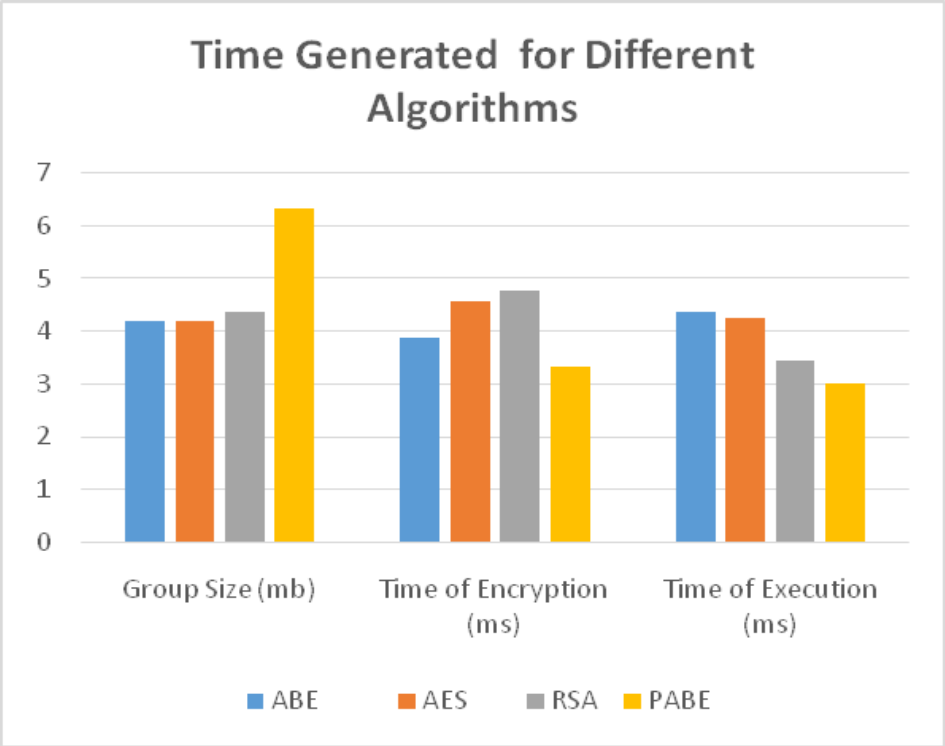

Figure 5: Encryption Time Trends Depending on Attributes

Table 3: Oauth 2.0 Identity Server 5.8.0 Overall Throughput

Concurrent Users	Throughput (Request/Sec)
1	4300
2	4200
3	4180
4	4100
5	4000

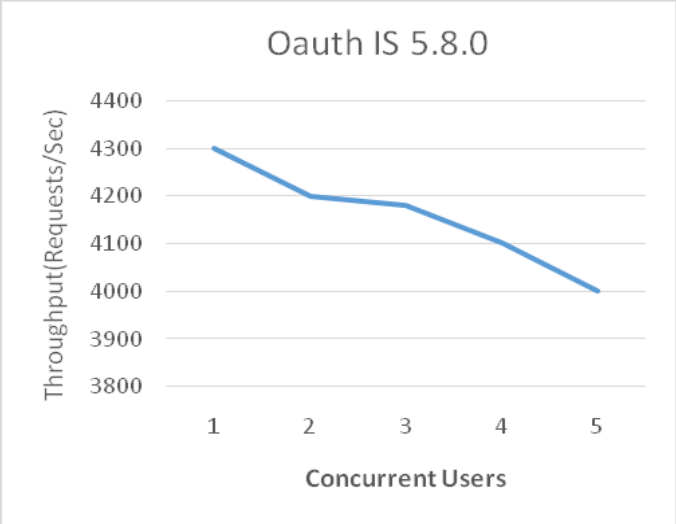

Figure 6: Oauth 2.0 Identity Server 5.8.0 Client Credentials Grant Flow

Table 3 and Figure 6. Depicts the 'grant', ideal for machine-to-machine Authorisation for a client to place the requests to a proposed system without the need of user's permission. Of course, it should be ascertained that only the authenticated clients are provided the grant. OAuth 2.0 Client credentials grant flow depicts a behaviour similarity to imply grant having throughput 5.8.0.

Table 4: Different Encryption Algorithm Performance Analysis

Techniques	**Accuracy**	**Recall**	**Mean Absolute Error**
Progressive Attribute Based Encryption	0.99	0.66	0.52
Attribute based Encryption algorithm	0.82	0.95	0.93
RSA (Rivest–Shamir–Adleman) algorithm	0.89	0.84	0.81
Advance Encryption Standard Algorithm	0.92	0.72	0.62

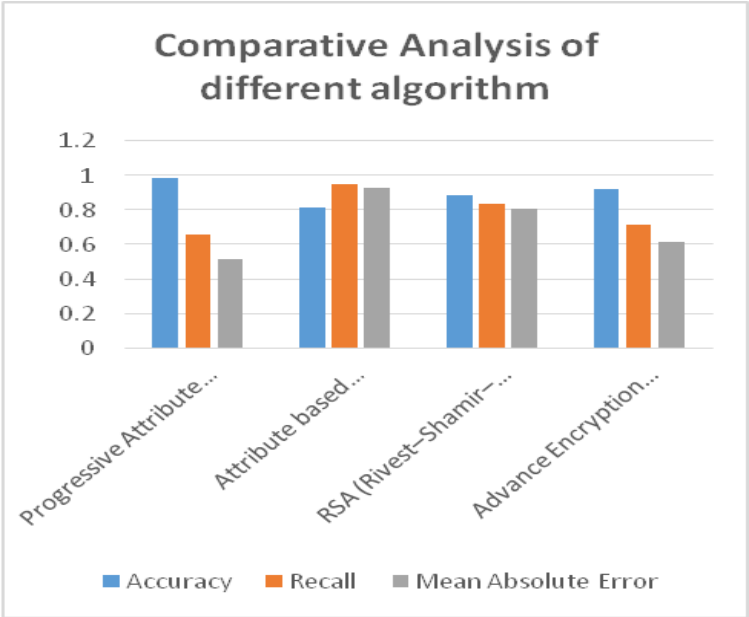

Figure 7: Comparative Analysis of Different Encryption Algorithms

There is performance evaluation of the cryptographic algorithms through multiple algorithms. The prevailing methods yield low accuracy and a high error rate. Table 4, Figure 7 illustrates the proposed PABE (Progressive Attribute Based Encryption) algorithm, depicting high accuracy but having low error rate and recall.

5 Conclusion

There is recommendation of a robust and secured cloud framework that ensures safe data access, security and data integrity. The E-health care data comprises of critical and sensitive records pertaining to the user's personal details, security, authorisation and even the user's authentication info. Hence, it's highly demanding that the cloud information remains highly secure and that there is efficiency and performance of the data so that the cloud storage and services remains trustworthy and safe. For fulfilling the above needs as per the user's satisfaction, a novel system has been proposed that is founded on the techniques of encryption, authentication, and authorization. The system strongly enforces that the data access is granted only to the authorized users' whereas the encryption algorithm is responsible for validating the data integrity amidst the cloud during any data exchange. It's evident from the output generated that the proposed light weight system is highly trustworthy, efficient and stable when handling and managing eHealth care information residing within the cloud storage.

References

[1] Yigzaw, K.Y., Michalas, A., & Bellika, J.G. (2016). Secure and scalable statistical computation of questionnaire data in r. *IEEE Access*, *4*, 4635-4645.

[2] Paladi, N., Gehrmann, C., & Michalas, A. (2016). Providing user security guarantees in public infrastructure clouds. *IEEE Transactions on Cloud Computing*, *5*(3), 405-419.

[3] Yigzaw, K.Y., Michalas, A., & Bellika, J.G. (2017). Secure and scalable deduplication of horizontally partitioned health data for privacy-preserving distributed statistical computation. *BMC medical informatics and decision making*, *17*(1), 1-19.

[4] Dowsley, R., Michalas, A., & Nagel, M. (2016). A report on design and implementation of protected searchable data in iaas. *Technology Representatives, Swedish Institute of Computer Science (SICS)*.

[5] Michalas, A. (2016). Sharing in the rain: Secure and efficient data sharing for the cloud. *In IEEE 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, 182-187.

[6] Grassi, P.A., Nadeau, E.M., Galluzzo, R.J., & Dinh, A.T. (2016). NIST Internal Report 8112 (Draft) Attribute Metadata.

[7] On January 13, 2016, the Russian Data Protection Authority (Roscommandzor) released its plan for audits this year to assess compliance with Russia's data localization law, which became effective on September 1, 2015.

[8] Li, Q., Zhu, H., Ying, Z., & Zhang, T. (2018). Traceable ciphertext-policy attribute-based encryption with verifiable outsourced decryption in ehealth cloud. *Wireless Communications and Mobile Computing*, *2018*.

[9] Sonya, A., & Kavitha, G. (2020). Securing the Healthcare Data with Blockchain Technology. *International Journal of Advanced Science and Technology*, *29*(4), 9474-9481.

[10] Sonya, A., & Kavitha, G. (2020) Encrypting Healthcare Data in Cloud Using Cryptographic Algorithms. *Test Engineering and Management*, *83*, 26722-26731.

[11] Hahn, C., Kwon, H., & Hur, J. (2016). Efficient attribute-based secure data sharing with hidden policies and traceability in mobile health networks. *Mobile Information Systems*, *2016*.

[12] Yu, G., Cao, Z., Zeng, G., & Han, W. (2016). Accountable ciphertext-policy attribute-based encryption scheme supporting public verifiability and nonrepudiation. *In International conference on provable security*, 3-18. Springer, Cham.

[13] Zhang, R., Hui, L., Yiu, S., Yu, X., Liu, Z., & Jiang, Z.L. (2017). A traceable outsourcing cp-abe scheme with attribute revocation. *In IEEE Trustcom/BigDataSE/ICESS*, 363-370.

[14] Yang, Y., Liu, X., Deng, R.H., & Li, Y. (2017). Lightweight sharable and traceable secure mobile health system. *IEEE Transactions on Dependable and Secure Computing*, *17*(1), 78-91.

[15] Luo, E., Wang, G., Tang, K., Zhao, Q., He, C., & Guo, L. (2018). Attribute-Based Traceable Anonymous Proxy Signature Strategy for Mobile Healthcare. *In International Conference on Information Security Practice and Experience*, 495-505. Springer, Cham.

[16] Jiang, Y., Susilo, W., Mu, Y., & Guo, F. (2016). Ciphertext-policy attribute-based encryption with key-delegation abuse resistance. *In Australasian Conference on Information Security and Privacy*, *Springer*, *Cham*, 477-494.

[17] Hahn, C., & Hur, J. (2016). Constant-size ciphertext-policy attribute-based data access and outsourceable decryption scheme. *Journal of KIISE*, *43*(8), 933-945.

[18] Teng, W., Yang, G., Xiang, Y., Zhang, T., & Wang, D. (2017). Attribute-based access control with constant-size ciphertext in cloud computing. *IEEE Transactions on Cloud Computing*, *5*(4), 617-627.

[19] Helil, N., & Rahman, K. (2017). CP-ABE access control scheme for sensitive data set constraint with hidden access policy and constraint policy. *Security and Communication Networks*.

[20] Wang, G., Lu, R., & Guan, Y.L. (2018). Enabling efficient and privacy-preserving health query over outsourced cloud. *IEEE Access*, *6*, 70831-70842.

[21] Manfredi, S., Ceccato, M., Sciarretta, G., & Ranise, S. (2022). Empirical Validation on the Usability of Security Reports for Patching TLS Misconfigurations: User-and Case-Studies on Actionable Mitigations. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *13*(1), 56-86.