International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Secured Authentication Using ECC Based Fractal Fuzzy in Cloud

A. Ahadha Parveen and P. S. S Akilashri

Submitted: 20/12/2023 **Revised**: 31/01/2024 **Accepted**: 10/02/2024

Abstract: In this paper, the study uses a novel design of the fractal fuzzy model in devising the secured authentication process via Elliptic Curve Cryptography (ECC). This model assists in improving the process of authentication in distributed cloud systems. The study uses attributed based data segregation that is developed using the preference of the data owners or users. Here, the priority is offered to sensitive data rather than non-sensitive data. After the grouping of the sensitive information based on the attribute, these subgroups are encrypted via group keys. Such encrypted information is then merged with the attributes that are of a non-sensitive type and then it is uploaded to the distributed cloud environment. The simulation is conducted in a cloudsim simulator to test the efficacy of the model against various types of attacks. The results of the simulation show that the proposed model performs with minimal computational complexity, storage space and processing time than the existing authentication models. Further, it offers an increased rate of security over sensitive and non-sensitive information than other methods.

Keywords: *Fractal Fuzzy Model, Elliptic Curve Cryptography, Authentication, Distributed Cloud Systems*

1. Introduction

The Infrastructure-As-A-Service (IaaS) model of cloud computing makes it possible to store enormous volumes of data dependably at a lower overall cost [1]. IaaS reduces the costs associated with maintaining infrastructure and enables management to be more effective. The use of the internet as a medium for the transaction of user data is becoming increasingly common. These processes take care of a diverse range of data types and degrees of sensitivity [2].

In the past, users' personally identifiable information was stored on the devices they owned and retained on their premises. When compared to using a cloud storage system provided by a third party, the use of this on-premise storage technique provided a higher level of data protection [3]. Cloud service providers (CSP) who are not affiliated with the company providing the cloud storage space are the ones responsible for the data stored there. As a direct consequence of this, information kept in the cloud is vulnerable to significant security threats [4].

When it comes to businesses in the healthcare and finance industries, data security is of the utmost significance when utilising cloud-based services. This is because these companies deal with sensitive information such as personal identification numbers (PINs), biometric information, etc. [5]. The significant volume of data and the storage of crucial information on third-party sites make cloud storage systems susceptible to unauthorised access [6].

Department of Computer Science, National College (Affiliated to Bharathidasan University), Trichy, Tamil Nadu, India, 620020

Cloud storage systems are vulnerable to illegal access due to the high volume of data. User data is currently being used for a variety of objectives by a broad variety of people, including the improvement of people's enterprises, the conducting of research, and the provision of improved services to customers [7]. As a consequence of this, the corporation is required to make the data usable to both internal and external members of the organisation without jeopardising the data owner's right to privacy. In this work, both sensitive and non-sensitive attributes are proposed to meet this condition with the knowledge of the data owner (DO) [8].

The most prevalent approaches to data security and classification, respectively, are the utilisation of data classification models that includes symmetric/asymmetric encryption methods [9]. These methods are not suitable for cloud storage since the accuracy of the classification technique is dependent on the user data attribute and training data. In a similar line, on-premises storage locations benefit from conventional symmetric and asymmetric encryption technologies, but cloud storage systems do not profit from these approaches [9]. Because of this, cloud-based secure data storage employs a form of attribute-based encryption (ABE) [10].

To provide effective access control and maintain the confidentiality of user information, cloud-based data often makes use of several different ABE encryption techniques. Among them are encryption methods such as role-ABE, key-policy ABE, ciphertext policy ABE, etc. The level of protection provided by ABE is proportional to the key values, attributes, or roles that are utilised throughout the encryption process [11].

Therefore, techniques that utilise selective attribute encryption are utilised to better protect particular properties as opposed to the whole attribute set. In addition, data owners are ready to share their information with approved users so that they can benefit from an improved level of service provided by the service providers themselves. The extent to which each user is willing to participate varies and this indicates the need for a security model that should offer the data owners the choice of security for their sensitive information [12].

Encryption's major purpose is to provide SI with efficient data access control, privacy protection, and integrity protection, and this is also its primary goal. However, current security solutions have a few drawbacks, including longer encryption times, a similar level of security for all characteristics, encryption and decryption that depend on a single key, non-involvement of the DO, and inter-organisational members [13]. These drawbacks make it difficult to implement these solutions. If the key is stolen or otherwise compromised, this could result in major issues, including the disclosure of confidential information [14].

When compared to the amount of time it took to encrypt a modest quantity of data using traditional security methods such as RSA, the amount of time it takes has climbed tremendously [15]. The Message-Digest 5 (MD5) algorithm is used to expedite the encryption process for Advanced Encryption Standard (AES) data. The secrecy of the encryption key is necessary for the efficacy of the AES encryption method. A communication that has been encrypted can be transmitted to a receiver who is aware of the user identity; in this case, the recipient will have access to a secret key that can be used to decrypt the message. Cloud-based data storage systems have a primary focus on the management and monitoring of data, as well as the management and security of stored data. Because cloud-based data storage relies on cloud service providers to maintain client records, these providers are tasked with this responsibility. As a direct consequence of this, cloud service providers are in complete command of any personally identifiable information about their customers. As a direct consequence of this, DO does not have any control over their data, and it can be accessed by anyone [16]. As a result, this paper suggests data storage and security that is based on DO controls.

Some of the shortcomings of the present security systems include the following:

- When it comes to data storage on the cloud, the ABE model offers less confidentiality as well as reduced levels of access control and monitoring for SI.
- A higher cost associated with communication and computational cost as well as a higher process overhead because all attributes must be encrypted and decrypted.
- The lack of participation by DO members as well as members of other organisations
- There is a possibility that adversaries from within the organisation will be able to enter SI.

Partition-based security is becoming increasingly popular as a novel approach to the protection of sensitive and confidential data in the modern era. In a similar vein, some aspects do not require any form of protection. If security measures are imposed across all attributes, authorised users will be responsible for increased processing costs [17].

As a consequence of this, attributes of the DO have to be segmented into SI and NSI, and different security methods need to be implemented for SI. Therefore, a suitable classification model is utilised to classify the data of DO. The accuracy of such classification that is already in existence is affected by the training set, therefore the model is selected based on the preference of DO while segmenting the SI [18]. To resolve this matter, the MRFC method will be utilised.

In this paper, the major contributions are given below:

- The owner of the data decided against employing algorithms for machine learning and instead chose to categorise sensitive attributes (SI) and non-sensitive information (NSI) instead.
- Make use of the sensitive attribute encryption rather than encrypting the entire attribute.
- To expedite the encryption process without jeopardising the privacy of the person who originally owned the data,
- To decrypt and gain access to only a subset of the characteristics that are required

2. Related Works

The combination of CoAP/UDP and DTLS was proposed by Villaverde et al. [19] as a solution for achieving reliable session negotiation, verification, and packet exchange across various devices. UDP is unreliable since it fails to have a specified mechanism for establishing a reliable connection between two devices. This instability is caused by the absence of a defined mechanism. There is no way to convert DTLS packets into TLS ones in a straightforward manner. The authors have implemented the 6LoWPAN Border Router (6LBR), which is a proxy for a direct mapping between CoAP and HTTP, to address these challenges.

According to Schneider et al. [20], TCP/UDP and TCP/UDP can be used in conjunction with Service

Oriented Architecture (SOAP) to ensure that communication with the server is kept private. When it comes to implementing web services, SOAP is more expensive than CoAP due to the broad data representation and transport mechanisms it offers, as well as the numerous cross-domain protocol capabilities it possesses. Because of this, SOAP cannot be used by IoT networks. Using a combination of CoAP/UDP and an effective XML exchange method like EXI is one way to cut down on the payload size of limited IoT devices. This is technically possible.

Bhattacharyya et al. [21] developed a model where DTLS uses a pre-shared, public key or certificate model. The first mode is the choice that has the least amount of overhead because it employs an asymmetric key encryption strategy. Because it does not enable lightweight multicast security, DTLS presents a significant challenge for IoT networks. This is another serious issue.

Granjal et al. [22] developed employing IPsec protocols in conjunction with the X.805 security standard as an alternative to DTLS in the secure implementation of CoAP. It is a fact that IPSec/X.805 is not capable of meeting the requirements for security that are imposed by CoAP. This is the case for several reasons, including the following: the limited space and complexity of IPSec; and the lightweight reliability over UDP, when a message is forwarded.

Researchers like Johnson et al. [23] and Ray et al. [24] have proposed using Wireless Transport Layer Security (WTLS) protocol. These researchers have criticised the functionality of IPSec in wireless communication. WAP is typically used on mobile phones, personal digital assistants (PDAs), and other devices that have limited computing capability. The utility of WAP is limited due to its functional complexity as well as concerns linked to WTLS. These issues include a lack of end-to-end security as well as a man-in-the-middle attack. These limitations can be circumvented with the use of the CoAP protocol, which also helps to cut down on bandwidth consumption.

According to Rahman and Shah [25] and Raza et al. [26], the following four security modes: CoAP/UDP paired with encryption techniques, DTLS/IPSec can be utilised to offer confidentiality, integrity, authentication, and non-repudiation:

NoSec mode does not provide any type of security service to the user. Utilizing symmetric keys instead of the traditional two-pre-shard key is another option that is available with this strategy. Because public keys are used for authentication in this mode rather than digital signatures, there is no need for an authentication certificate to be used. A DTLS session can be initiated with the use of a pre-shared set of keys for the devices that will be talking with one another. When validating certificates in this manner, asymmetric keys and the X.509 certificate standard are both utilised as tools. On the other hand, ECC is a form of public-key cryptography that enables users to choose between the Certificate mode and the Raw Public Key mode when encrypting data. A preshared key, which is integrated with a CoAP environment, can be used to construct a system that is based on a preshared key, which is abbreviated as PSK. Raw Public Key mode is an option for DTLS when it comes to communicating with servers. Because of this, DTLS does not make it possible to send multi-cast messages between two hops or objects, which is a limitation of the security provided by CoAP.

Urkia et al. [27] recommended using libraries from a variety of programming languages and environments, including Java, Python, and JavaScript, to put into practice CoAP. In terms of their performance, the SMCP and SMCOAp libraries are among the most efficient when compared to other libraries. Alabas et al. [24] predicted an evaluation that would be based on the many different architectures that are currently accessible regarding vulnerabilities, security, and communication with servers.

According to Albalas et al. [28], a comparison of ECC and RSA CoAP was conducted regarding the length of the messages, the security services provided, and the residual energy. This evaluation used three factors. The CoAP that uses ECC has a 47% higher energy efficiency than the CoAP that uses RSA. This is because ECC has a smaller key size. Even with ECC, there are still obstacles to overcome in multicasting, asynchronous data transfer, and CoAP key management. These discoveries served as the impetus for the development of the ECC-CoAP protocol, which eliminates the disadvantages described above to an almost fully satisfactory degree.

The security issues are maintained by encrypting necessary CoAP requests and answers using ECC. An IoT controller is responsible for managing all of the traffic on this wireless network. Nevertheless, it turns out that the approach [29] has some significant problems with the management of the CoAP.

Dey and Hossain [30], who advise using the LESS protocol to establish session keys for smart home networks, have demonstrated that existing LESS protocols are susceptible to relevant security threats. As a result, they recommend using the LESS protocol.

3. Proposed Method

In the last few decades, the understanding of the geometric complexity of objects has made significant strides thanks to the development of fractal theory. In financial and economic user data, for instance, one can observe the

presence of a fractal structure. The following is an illustration of one definition of a fractal dimension:

$$d_{r\to 0} = \lim \frac{\left[\ln N(r)\right]}{\left[\ln\left(\frac{1}{r}\right)\right]} \quad (1)$$

There are a total of $N(r)$ boxes covering a particular item, with r indicating the size of each box. The study conducts a normalisation of numeric values in fractal dimension by may counting the total boxes covering an item that consists of different values of r. Here, the computation of finding d is conducted via least squares regression. This can be done to produce an estimate of the fractal dimension.

3.1. Fractal Dimension

The box-counting method is utilised on a random curve denoted by C. By applying the following equation, normalisation of the crisp value of the box dimension for any geometrical object. Performing a regression after initially counting the boxes that lie in the range of various r values.

$$\ln N(r) = \ln \beta - d \ln r \quad (2)$$

Estimation of the fractal dimension d can be done with the use of the least-squares method if the data is taken into consideration.

A fractal dimension is a useful tool that may be used to characterise any random object. To phrase it another way, the fractal dimension is a measurement of the geometric complexity of the thing being measured. In this study, the classification of the SI and NSI is accomplished by using the numerical present in the fractal dimension. This method of categorization is founded on the observation that the value in the fractal dimension is very close to one of the boundaries of the object in question and can be described as smooth. Even though this is the case, the value in the fractal dimension will be closer to two when the object boundary is rougher.

3.2. Fuzzy Logic Classification

The process of classification can be simplified by employing fuzzy logic, which divides the input space into granules of decreasing size. These granules can then be used to determine the primary characteristics shared by various users. After applying fuzzy classification over the user data, we are then in a position to create a fuzzy system that can act as a classification solution for the particular circumstance that is at hand.

When the study applies fuzzy clustering to the n items O_1, O_2,...O_N, the n pairs (X_i and Y_i) for all $i = 1,2,\ldots,n$ serve as the centres of each of the n clusters that can be produced as a result. Constructed based on these points as a foundation, the fuzzy system that follows is as follows:

If $X = x_1$ && $Y = y_1$ then Data = O_1

If $X = x_2$ && $Y = y_2$ then Data = O_2

If $X = x_n$ && $Y = y_n$ then Data = O_n (3)

The fuzzy system represented by Eq. (3) is capable of solving both types of problems because the fundamental building blocks of categorization and the prediction of user data are the same. To completely develop and implement the fuzzy system described in Eq.(2), it is necessary to construct membership functions for each fuzzy set in Eq.(3).

3.3. Proposed Fractal Fuzzy Logic

Let's consider an in-depth analysis of the difficulty that comes with categorising data in user data analysis. For the sake of convenience, we will designate arbitrarily long user data using the integers y_1, y_2,…,y_n. Before user data can be categorised, the underlying data must first be analysed, to extract recurring patterns and trends from the data.

Assume the user data is split into n different pieces, such as O_1, O_2,...O_N then we can create a fuzzy system. The estimated fractal dimensions of the objects O_1, O_2,...O_N in terms of their complexity is a new aspect that is taken into account by the hybrid technique.

In addition, the fuzzy system takes advantage of the fractal dimensions of linear (dim_1) and non-linear (dim_1) types and assigns the fuzzy values x_1, x_2,…,x_n and y_1, y_2,…,y_n to each of these dimensions, respectively. Both linear and non-linear methods of approximating the data take a different approach to the outputs of the dimensions.

Because of this, the study has decided to categorise the data using both forms to achieve higher levels of accuracy in our classifications. When employing fuzzy logic, a fuzzy user data classification is outlined using the form that is shown below.

If $dim_1 = x_1$ && $dim_2 = y_1$ then classification = O_1

If $dim_1 = x_2$ && $dim_2 = y_2$ then classification = O_2

If $dim_1 = x_n$ && $dim_2 = y_n$ then classification = O_n

In Equation, membership functions are required to be built for both fractal dimensions as in Eq. (4). For defuzzifying, this fuzzy system, the Mamdani approach and the centre of the region are utilised.

SI (fractal dimension), NSI (nonlinear fractal dimension), SI (nonlinear fractal dimension), and NSI (fractal dimension), are their own unique set of four inputs, which are denoted by FSI, NNSI, NSI, and FNSI, respectively. In this context, the concepts of low and high linguistic

values are utilised to represent the idea of little and huge dimensions, respectively.

Depending on the sensitivity of the data, the different levels of the high, medium, and low are defended. Existing data and the values produced from fractal dimensions are used as inputs for developing the rules in fuzzy systems. However, the approach can be used for several different time frames, and the classification of sensitive data may change depending based on the preference of the users in the current time frame.

Authentication based on User Attributes

Group-key-based sensitive attribute protection is the type of encryption that is used in private distributed clouds because it provides an additional layer of security. The SI and NSI are separated into different groups according to the privacy score values of several different features, and the D_O is in charge of supplying security preferences. In the proposed system that is outlined in Table 1, each participant stops a distinct function.

It is required that a value on the Likert scale (D_o) be assigned to each characteristic. The general administration will take this value and convert it to a value on the dichotomous scale (DSV), which will be used in the process of developing the response matrix $RD(i,j)$. The values for sensitivity (β) and visibility $V(i,j)$ are calculated by utilising the information obtained from $RD(i,j)$. The average value of the privacy score is what is utilised in the calculation of the threshold T. When compared to the threshold value, the PSV of an attribute is considered to be Satisfactory if it falls below that value.

The S_I is now encrypted by utilising the mechanism that was proposed, in contrast to the N_{SI} data, which is stored on the cloud in a plain-text format. This ECC based group key approach that has been recommended makes use of several symbols, which can be seen in Table 2. The preferences of D_o are determined by the current status of security. As a consequence of this, organisations that do not handle data are the only ones able to ensure the safety of the data.

The practice of conducting business online and exchanging data with other organisations is rapidly becoming the standard for many different types of organisations. Stringent security is required to protect a S_I while data is being transmitted between different organisations. A few of the components of the system that have been mentioned are Group Admin (G_A), G_{NA} and Cloud Service Provider (CSP). The uploading of $G(S_I)$ to cloud storage by the D_O is secured with encryption provided by Group Key (G_K). The G_A will send a request message to the CSP if they require information on D_O for their process. CSP is responsible for vetting authorization requests, after which it sends the key request to DO. Then the request is analysed by D_O and then it is encrypted by $G(S_I)$ and sent to G_A.

The GK was created by D_O, and they employ it in the encryption of their $G(S_I)$. By utilising this approach, no D_O data is shared with anybody else without first receiving D_O approval, and D_O is provided with the CSP transaction log records about all requesters. Because of this, the D_O exercises complete authority over and monitoring of their data. Another GN_A has been given the responsibility of deciding whether or not to offer the GA access to the DO data.

Sensitive Attributes Grouping

An Elliptic Curve Cryptography technique is utilised by ECC-GA to generate keys that correspond to the characteristics of the Elliptic Curve equation

$$y^2=(x^3+1+ax+1+b)\text{mod}p$$

This equation is used to determine the attributes of the elliptic curve. In ECC-G_A, the Diffie–Hellman key exchange method is utilised in conjunction with the key generation process to accomplish the task of key exchange.

Properties.

The following is a list of the three distinct types of groups that exist:

- The term secret attributes (S_I) refers to characteristics of a person or thing that should not be disclosed to other people or things.
- This is the collection of attributes that the G_{Ai} has the potential to make available to you.
- It is the ubiquitous $G(S_I)$ that can be found in several different G_A.

As mentioned in Algorithm 1 of the text, the technique for grouping S_I depends on access to user information. $R_{\text{eq}}(\text{G}_{\text{Ai}}\text{G}_{\text{Ai}}) \in \{A_1, \ldots, A_n\}$ is the requirement for collaboration between organisations that was received from the GA. In this scenario, the property $R_{\text{eq}}(\text{G}_{\text{Ai}}\text{G}_{\text{Ai}})$could belong to either the S_I or the NS_I.

If $A_1,\ldots, A_m \equiv S_I$, then $A_{m+1}, \ldots, A_n \in NS_I$ becomes $A_1, \ldots, A_m \in G_{Ai}G_{Ai}(G(S_I))$, otherwise $A_{m+1}, \ldots, A_n \in NS_I$ becomes $A_1,\ldots, A_m \in G_{Ai}+1G_{Ai}+1(G(S_I))$.

Similarly, the approach is applied to the S_I grouping that is determined by the remaining G_A requirements. Certain traits are shared by everyone in this predicament. Some criteria are shared by both the G_A and the S_I, and these are denoted by the notation $\text{C}(\text{G}(S_\text{A}))$. Below are the qualities obtained by subtracting $\text{GAi}+1\text{GAi}+1(\text{G}(S_\text{A}))$ from $\text{C}(\text{G}(S_\text{A}))$. The completion of this process will result in the creation of an organization-required attribute group as

well as a D_O private attribute group. It is now time to start the encryption process with the $G_{AiGAi}(G(G_A))$ as it has reached the appropriate point in time.

Group Key Generation

Key generation refers to the process of creating GKs for encryption. This procedure is necessary for secure communication. The key is generated through the usage of elliptic curve cryptography as well as the ECC numbers. Using Algorithm 3, and selecting an elliptic curve of the form

$$y^2=(x^3+1+ax+1+b)\text{mod}p.$$

The beginning and ending values of the random number generation process can be obtained. The GK generation task states the starting parameters "*P*, *n*, and *Q*" as a consequence of these values (initial, final, and total values).

Preliminaries

Bilinear Map: One way to think about the two groups (G, +) and (G,.) and P_0 is as cyclic groups with the shared initiator *G* and similar prime order (*P*). If $e(G\times G)\rightarrow G_1$ is found to be true during the process of bilinear mapping, then it possesses the following properties:

- **Non-degeneracy**: The condition $e(P_0,P_0)\neq 1$ for non-degeneracy has been satisfied.
- **Bilinear**: Two different approaches could be taken here: $e(P_x,P_y)=e(P_y,P_x)=e(P,P)^{xy}$
- **Computability**: It is the case that $e(P_x,P_y)$ is true for $P_1, P_2 \in G$.

Bilinear Diffie–Hellman Decision:

The term polynomial time refers to the amount of time required by an algorithm that contains *n* stages (q,G,G_1,e). The numbers *n*, *G*, G_1, and *e* were used in the process of selecting a prime number that will be referred to as q. Each probabilistic polynomial-time distinguisher (*D*), as well as every distinguisher (q,G,G_1,e) formed by *n*, is considered to be a negligible function, and the definition of neg is as follows:

$$P_r(D(G,G_1,q,e,P_x,P_y,P_Z,e(P_0,P_0)^{xyz}=1) = (P_r)^{xyz}$$

$$P_r(D(G,G_1,q,e,P_x,P_y,P_Z,e(P_0,P_0)^{w}=1) = (P_r)^{w}$$

$$|(P_r)^{xyz} - (P_r)^{w}| \leq \text{neg}(n),$$

where *x*, *y*, *z*, and *w* are the four identical components of F_P and P_0 is a random generator of *G*. Included in the system that is being proposed are operations such as *Setup*, KeyGen, *Encryption*, and *Decryption*.

Setup: The global parameters are generated by the GNA for the (P_u,P_r) generation for each DO and GA. To create the GK, the inputs that are used are the EC points (*P*,*Q*), as well as the base point (*G*) of the elliptic curve. When it comes to getting a new user set up and operational, there are a few different G_A and D_O steps that need to be completed. Throughout the process of setting up a user, F_P is utilised to ascertain both the G_A ID and the D_O ID. These IDs are kept up to date in the cloud to facilitate G_A and D_O verification.

KeyGen(): Each D_O determine (P_u,P_r) by applying the ECC-GA methodology to their calculations. The ECC numbers *P* and *Q* are used in the calculation of the P_r. Each D_O can generate an "n+1" G_K for the encryption if they maintain a record of all of the different GKs that they have generated over time.

Encrypt: The encryption method known as $E(G_{Ai}G_{Ai}(G(S_I))) \leftarrow \text{Enc}(G(S_I))$ is used by the D_O to encrypt a group of S_I.

Decrypt: This method employs a GA to decrypt the string $E(G_{Ai}\ (G(S_I)))$.

Add/Revokeuser(): The add user and revoke user operations are both carried out via a D_O.

The security of a cryptographic technique can be improved by increasing the unpredictability of the integers that are used in the procedure. A strategy for selecting random numbers is proposed in a new method that makes use of a modified version of ECC cryptography. To establish the beginning and ending points of an ECC series, it is necessary to find the solution to a simple equation involving an elliptic curve. The ECC numbers that are produced are put to use as a source of information in the generation of random numbers. The Rand () function is used to create random numbers based on the ECC sequence. This is done in place of picking a private key based on an elliptic curve as the basis. When choosing a private key using this method, it will be more challenging for an adversary to determine which key is a private one. We chose to use the ECC number as our private key because it is impossible for a potential attacker to determine which set of sensitive attribute encryption it is being used for. This technique is used by each DO to generate their private keys, which are then used in the construction of the $n + 1$ group keys. As a consequence of this, the proposed method generates private keys with a greater degree of unpredictability in comparison to the conventional elliptic curve-based method. In the recently developed method, the number of values that are utilised to build a set of group keys is determined by the individual using the method.

The ECC sequence, $F[n] \in \text{EC}[P\ldots. Q]$, is used in the ECC-GA that has been proposed. The rand() function is used to select a value at random from $F[n]$ and store it in A. The P_r value for each DO is determined by using its

$A[n]$ value as the basis. It is possible to determine the P_r of a D_O by using the following equation:

$$P_{r_i} \leftarrow \left(QA[i] + P + \left(\frac{F[n]}{A[n]} \right) \right)$$

The values that are created for the P_r variable are Saved in an array called $K[n]$. The product P_u is obtained by multiplying P_r by G. Once this objective has been met, $G_{Ki} \leftarrow P_{uA} * P_{rB}$ is the next step. To encrypt the G, several g_{ki} that correspond to it are generated and used (S_I). To produce a key, the algorithm first determines whether or not the GA is greater than the O_i. Returns to G_A In all other cases, O_i will return the G_K, which is composed of tuples:

$$G_K \in (P, Q, A[i], F[i], P_r, P_u, B)$$

Sensitive Attribute Encryption

The G is encrypted with the help of a suitable $G_K(S_I)$. Communication sent over Gmail is encrypted using a brand-new encryption mechanism (S_I). The number of organisations that take part in a procedure determines the total number of ciphertexts (C) that are generated by the procedure.

When performing an encryption procedure, using the key G_{Ki} is functionally equal to using the key $(G(S_I)) \in G_{Ai}(G(S_I)), G_{Ki}$. The technique is carried out in the same manner for $G(S_I)$ that have different G_K. The N_{SI} has now been integrated, and the encrypted $G(S_I)$ has been transferred to the cloud for safekeeping thereon.

Group Key Sharing

If a certain $G(S_I)$ is required, the P_u of D_O is consulted to locate the G_{Ki}. In both D_O and G_A, the P_u can be found in sentences that have the same meaning. When a G_A is necessary to gain access to a specific G, the value of P_r is multiplied by the $D_O(P_u)$ to acquire the $G_K(S_I)$. The encrypted G can be decrypted with the help of the G_K (SA).

Merging Attributes and Transfer

The General Authority (G_A) sends a request for authentication to the CSP, and the CSP verifies the identity of the G_A. If the verification is found successful, the encrypted $G(SA)$ will be sent. Deciphering the G requires the G_A to employ the relevant $G_K(S_I)$. The technique of combining and transferring $G(S_I)$ and N_{SI} information.

During the process of transferring data over the cloud, this property, $E(G(S_I))$, remains completely secure. After that point, access to E will only be granted to those individuals who have been validated by the G_A of the process G_{Ki}. In the proposed method, individual customers would not be sent to G_A; rather, only the desired customer details would be transmitted. This method cuts down not just on the amount of time required to transfer and decrypt data, but also on the amount of money required to send unnecessary data.

Decryption

The SI encryption and decryption processes are related to one another in a manner that is inverse to one another. Before a G_A can decrypt and access the G, its User ID must first be validated to ensure that it is not on the list of revoked $G_A(S_I)$. CSP will request to D_O when a G_A has not been revoked. After D_O validates its authenticity, CSP will deliver the necessary.

The complete data set does not need to be decrypted; rather, only the properties that are necessary to fulfil the needs of the specific application are accessed. This task requires a particular G_K from both the G_A and the D_O to successfully decrypt the information. If the $G_K(G_A)$ has been revoked by the organisation, it will not be possible to find them. The list is no longer accessible as a result of the revocation process, which involved the removal of G_A-related G_K. A revoked G_A will prevent a decryption operation from gaining access to a $G(S_A)$. For the G_A to decode the information, it must calculate G_{Ki} based on P_{ri}.

$$P_{ui} \leftarrow P_{ri} * G$$

If $P_{ri} \in F_P$, then $P_{ui} \in F_P$.

Now, $G_{Ki} \leftarrow P_{rA} * P_{uB}$

If the person making the request has their FP privileges revoked, P_{ri} and P_{ui} do not belong to F_p. They are no longer permitted to utilise the G because the G_A has been eliminated (S_I).

User revocation

The cloud storage must be updated with the user, ciphertext, and G_K updates whenever a G_A is either removed from the process or added to it to guarantee the system's full security. Whenever the G_A is revoked, the specific G encryption is performed using the new G_K, which also generates new encryption based on the new $G_K(S_I)$. The following phases make up the procedure of revocation:

- The User ID of the G_A should be removed from the CSP, and the change should be made dynamically.
- Make sure that the revoked G_A user ID is added to the list of users who have had their access revoked so that any future abuse can be avoided.
- It is necessary to pick a number at random from the ECC series, and that number is R_1.
- Produce a brand-new key pair consisting of a P_r and a P_u for use in the development of a G_K.

- The new ciphertext for the user whose $G(S_A)$ privileges have been removed is now being generated and uploaded to the cloud.

4. Results and Discussion

Encryption, decryption, and overall processing time are evaluated for the RSA (Basic) algorithm, together with its two variants, and the ECC algorithm. The first kind of RSA is called RSA with CRT, while the second variant is called Multi-Prime RSA. For this research, sample OTP message data consisting of 27 bits and 270 bits, respectively were utilised to test the time efficiency of these various approaches.

Experiments with the proposed ECC model with 1024/2048/3072 bits for RSA and 160/224/256 bits for ECC. These bit lengths represent the modulus. The corresponding programming code was written in C and tested on a laptop with a dual-core Intel Pentium processor, 533MHz processing speed, 1MB of L2 cache, 2GB of DDR2 memory, and the Microsoft Windows operating system.

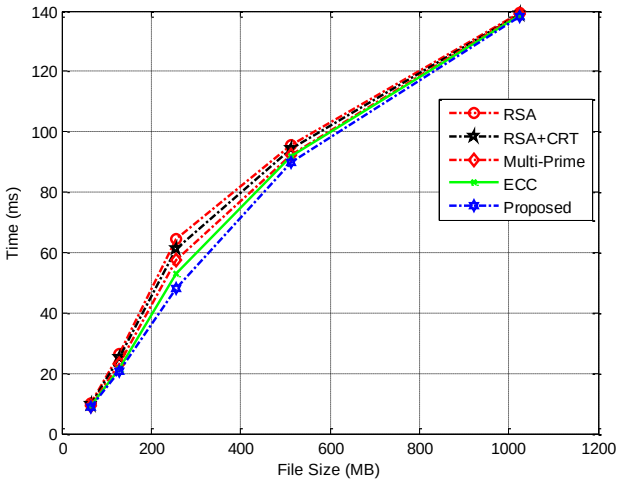

Fig 1: Encryption time

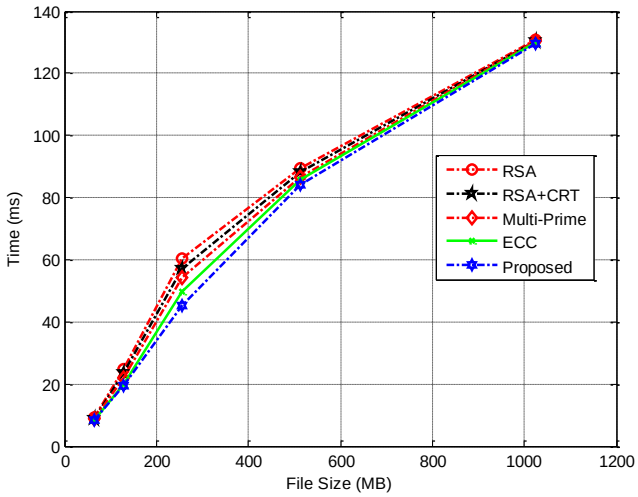

Fig 2: Decryption time

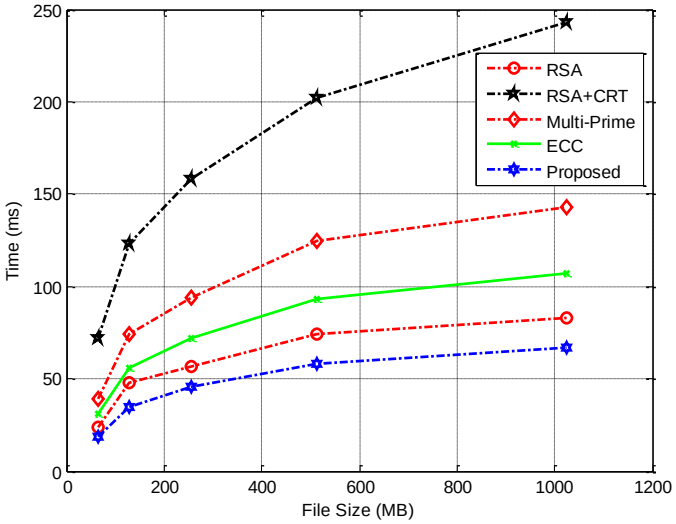

Fig 3: Computational Time (ms)

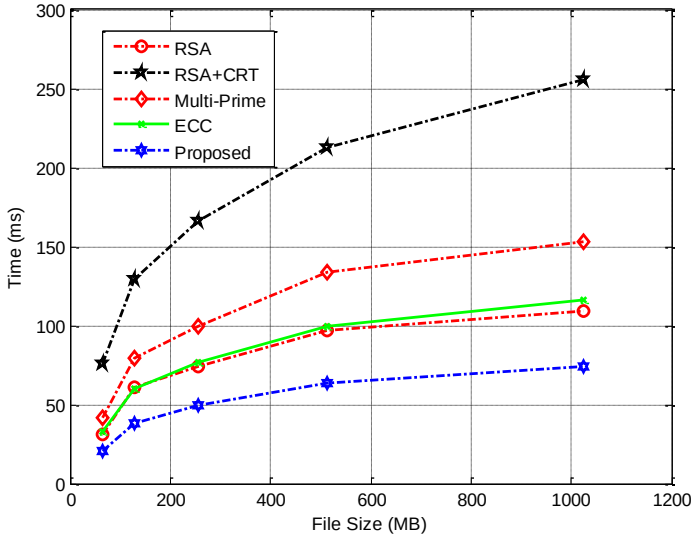

Fig 4: Communication Time (ms)

It has been demonstrated that RSA (Basic) takes significantly more time than RSA, ECC, and the proposed method as in Figures 1 and 2. According to Figures 3 and 4, ECC performs better in terms of operational efficiency than RSA and both of its versions.

5. Conclusion

Using a unique fractal fuzzy model, the researchers in this paper devise an ECC-based method for securely authenticating users. Using this concept, distributed cloud systems can improve the authentication process. An attribution-based data segregation method is used in the study, which is based on user preferences. In this case, sensitive data is given precedence over non-sensitive data. Group keys are used to encrypt the subgroups formed once the sensitive data has been grouped according to the attribute. Encrypted data is subsequently combined with non-sensitive attributes and uploaded to the dispersed cloud environment. Cloudsim simulator is used to assess the model's ability to withstand various forms of attacks. Simulated findings show that the suggested model performs better than existing authentication models in terms of computational complexity, storage space, and processing time. Other approaches cannot compete with its higher level of security for both sensitive and non-sensitive data.

References

[1] Narayanan, U., Paul, V., & Joseph, S. (2020). A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment. *Journal of King Saud University-Computer and Information Sciences*.

[2] Falmari, V. R., & Brindha, M. (2020). Privacy preserving cloud based secure digital locker using

Paillier based difference function and chaos based cryptosystem. *Journal of Information Security and Applications*, *53*, 102513.

[3] Manivannan, D., & Brindha, M. (2022). Secure Image Cloud Storage Using Homomorphic Password Authentication with ECC Based Cryptosystem. *Advances in Systems Science and Applications*, *22*(1), 92-116.

[4] Chen, Y., & Chen, J. (2021). A secure three-factor-based authentication with key agreement protocol for e-Health clouds. *The Journal of Supercomputing*, *77*(4), 3359-3380.

[5] Wang, F., Xu, G., Xu, G., Wang, Y., & Peng, J. (2020). A robust IoT-based three-factor authentication scheme for cloud computing resistant to session key exposure. *Wireless Communications and Mobile Computing*, *2020*.

[6] Giri, S., Su, J., Zajko, G., & Prasad, P. W. C. (2020, November). Authentication method to secure cloud data centres using biometric technology. In *2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA)* (pp. 1-9). IEEE.

[7] Khan, N., Zhang, J., & Jan, S. U. (2022). A Robust and Privacy-Preserving Anonymous User Authentication Scheme for Public Cloud Server. *Security and Communication Networks*, *2022*.

[8] Kakkar, A. (2020). A survey on secure communication techniques for 5G wireless heterogeneous networks. *Information Fusion*, *62*, 89-109.

[9] Qiu, S., Wang, D., Xu, G., & Kumari, S. (2020). Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices. *IEEE Transactions on Dependable and Secure Computing*.

[10] Ma, R., Cao, J., Feng, D., Li, H., Niu, B., Li, F., & Yin, L. (2020, May). A secure authentication scheme for remote diagnosis and maintenance in Internet of Vehicles. In *2020 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1-7). IEEE.

[11] Srinivas, J., Das, A. K., Wazid, M., & Kumar, N. (2018). Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things. *IEEE Transactions on Dependable and Secure Computing*, *17*(6), 1133-1146.

[12] Yuvaraj, N., Arshath Raja, R., & Kousik, N. V. (2021). Privacy preservation between privacy and utility using ECC-based PSO algorithm. In *Intelligent computing and applications* (pp. 567-573). Springer, Singapore.

[13] Sham, E. E., & Vidyarthi, D. P. (2022). CoFA for QoS based secure communication using adaptive chaos dynamical system in fog-integrated cloud. *Digital Signal Processing*, *126*, 103523.

[14] Meshram, C., Imoize, A. L., Jamal, S. S., Alharbi, A. R., Meshram, S. G., & Hussain, I. (2022). CGST: Provably Secure Lightweight Certificateless Group Signcryption Technique based on Fractional Chaotic Maps. *IEEE Access*.

[15] Kotha, S. K., Rani, M. S., Subedi, B., Chunduru, A., Karrothu, A., Neupane, B., & Sathishkumar, V. E. (2021). A comprehensive review on secure data sharing in cloud environment. *Wireless Personal Communications*, 1-28.

[16] Meshram, C., Lee, C. C., Meshram, S. G., & Meshram, A. (2020). OOS-SSS: an efficient online/offline subtree-based short signature scheme using Chebyshev chaotic maps for wireless sensor network. *IEEE Access*, *8*, 80063-80073.

[17] Tanveer, M., Zahid, A. H., Ahmad, M., Baz, A., & Alhakami, H. (2020). LAKE-IoD: Lightweight authenticated key exchange protocol for the Internet of Drone environment. *IEEE Access*, *8*, 155645-155659.

[18] Adhikari, S., & Karforma, S. (2022). A novel image encryption method for e-governance application using elliptic curve pseudo random number and chaotic random number sequence. *Multimedia Tools and Applications*, *81*(1), 759-784.

[19] Villaverde, B. C., Pesch, D., Alberola, R. D. P., Fedor, S., & Boubekeur, M. (2012, July). Constrained application protocol for low power embedded networks: A survey. In *2012 sixth international conference on innovative mobile and internet services in ubiquitous computing* (pp. 702-707). IEEE.

[20] Schneider, J., Kamiya, T., Peintner, D., & Kyusakov, R. (2011). Efficient XML interchange (EXI) format 1.0. *W3C Proposed Recommendation*, *20*, 32.

[21] Bhattacharyya, A., Bose, T., Bandyopadhyay, S., Ukil, A., & Pal, A. (2015, March). LESS: Lightweight establishment of secure session: A cross-layer approach using CoAP and DTLS-PSK

channel encryption. In *2015 IEEE 29th international conference on advanced information networking and applications workshops* (pp. 682-687). IEEE.

[22] Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, *17*(3), 1294-1312.

[23] Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). *International journal of information security*, *1*(1), 36-63.

[24] Ray, S., Biswas, G. P., & Dasgupta, M. (2016). Secure multi-purpose mobile-banking using elliptic curve cryptography. *Wireless Personal Communications*, *90*(3), 1331-1354.

[25] Rahman, R. A., & Shah, B. (2016, March). Security analysis of IoT protocols: A focus in CoAP. In *2016 3rd MEC international conference on big data and smart city (ICBDSC)* (pp. 1-7). IEEE.

[26] Raza, S., Helgason, T., Papadimitratos, P., & Voigt, T. (2017). SecureSense: End-to-end secure communication architecture for the cloud-connected Internet of Things. *Future Generation Computer Systems*, *77*, 40-51.

[27] Iglesias-Urkia, M., Orive, A., & Urbieta, A. (2017). Analysis of CoAP implementations for industrial Internet of Things: A survey. *Procedia Computer Science*, *109*, 188-195.

[28] Albalas, F., Al-Soud, M., Almomani, O., & Almomani, A. (2018). Security-aware CoAP application layer protocol for the internet of things using elliptic-curve cryptography. *Power (mw)*, *1333*, 151.

[29] Harish, M., Karthick, R., Mohan Rajan, R., & Vetriselvi, V. (2018, January). Securing CoAP through payload encryption: Using elliptic curve cryptography. In *International Conference on Communications and Cyber Physical Engineering 2018* (pp. 497-511). Springer, Singapore.

[30] Dey, S., & Hossain, A. (2019). Session-key establishment and authentication in a smart home network using public key cryptography. *IEEE Sensors Letters*, *3*(4), 1-4.