A Secured Data Storage Mechanism Using Baye's Theorem and Matrix for Effective Data Communication in Cloud

Nithisha J[1], Jesu Jayarin P[2]

[1] Faculty of Information and Communication Engineering, Anna University, India
[2] Department of Computer Science and Engineering, Jeppiaar Engineering College, India
nithisha.j@gmail.com, jjayarin@gmail.com

Abstract

In cloud, the data security is playing major role for ensuring the drastic improvement of the number of cloud users. For this purpose, many secured data storage mechanisms are introduced by the researchers in the past. However, the available mechanisms are consuming more time and also not achieved the required security. For fulfilling this gap, this paper introduces a new Baye's theorem and Matrix translation based secured data storage method to store the cloud user's data securely in effective manner in cloud. Moreover, a new Baye's theorem-based authentication scheme to access the encrypted data from the cloud database. The proposed secured storage method incorporates an encryption method called Elliptic Curve Cryptography and also applies the matrix translation method for performing encryption process effectively. In addition, the matrix transposition method is applied for performing decryption process over the encrypted text. This work applies base theorem for generating keys for the cloud users to access the encrypted data that are taken from cloud server. The experiments have been carried out to evaluate the performance of the proposed secured data storage and retrieval model and it is proved the efficiency and effectiveness with respect to high security level than the available methods.

Keywords: Baye's theorem, ECC, Encryption, Decryption and authentication

1 Introduction

Recently, the distributed services are emerging and essential for this fast internet era. Many distributed network models, infrastructures like pervasive network environment, autonomic network environment, cloud environment and distributed network environment, etc. are created and used for exchanging the data and resources. Even though, a Gap is available between the users and the environment due to the lacking of security and privacy preservation. The cloud computing is working based on computer networks in which the individual nodes are connected through internet that provides services for fulfilling the cloud user's requirements.

The main advantage of the cloud computing are flexibility, reliability and manageability. Moreover, it has economy, reliability, versatility and environment features on-demand. The client of a cloud can be used the available software tools in cloud based on requests and also can be deployed anywhere in the cloud / devices [2-3]. The basic cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a- Service (IaaS) that are providing services to the client through Cloud Service Provider (CSP).

Moreover, four types of cloud models such as Private Cloud, Public Cloud, Community Cloud and Hybrid Cloud are available to distribute the resources and it coordinates the Cloud admins. On the other hand, the cloud platform is facing lot of issues related to scalability, multi-tenancy and interoperability. The major issue is security in cloud that is expressed with different kinds of threats as a system that uses the internet networks including grid computing and embedded networks [4]. The security issue in cloud is worldwide accepted one and it is necessary to share the services and data. So that the security is very important in cloud and it must supply a safe link to the CSP and the cloud users. In this direction, many security mechanisms and protocols have been developed for ensuring the data transfer security on cloud network. For providing security, the cryptography is playing vital role and widely used in various cloud applications for secured storage and retrieval. Moreover, the data translation between plain text and cipher text is done in cryptography. In general, it is a software which is helpful for securing the data transfer and also ensuring the data availability in cloud [7].

In cloud, the confidentiality, integrity, availability, authentication and authorization are identified as key requirements for providing security to the users. The confidentiality is used to maintain the user's data and permit to access the data by the individual users alone.

*Corresponding Author: Nithisha J; E-mail: nithisha.j@gmail.com
DOI: 10.53106/160792642021072204012

The integrity is a commitment for ensuring the data is not changed and it is transmitted in cloud with the rights to repeat, modify and delete. The authentication is ensured the cloud user's integrity when permits to access the data and it is achievable with the help of their accounts. The availability means that the data is available with accessibility from anywhere. The authorization is guaranteed that to get the special details of the cloud users those are accessed the data in cloud.

Cryptography is used to provide the data security by encrypting the data and changed to non-understandable. This cryptography permits the data to encrypt and decrypt without the help of sender. Moreover, it is also provided the authentication to the cloud users. The existing networking technology is greatly enhanced and also required to send the limited volume of data through Internet. The cryptography technique is useful for avoiding the insecure communication on cloud and also supplies a best idea to provide the required security against the intruders. The mathematics are more helpful for performing the encryption and decryption processes. The matrix-based security mechanisms are also available in the literature [1]

The combination of cryptography and cryptanalysis is called as cryptology [2-3]. Generally, the sender is responsible for performing encryption using a secret key and the receiver node is capable of decrypting the encrypted data using a shared key which is secret. The cryptographic methods can be categorized into two such as Symmetric and Asymmetric key cryptography. In the symmetric key cryptography, similar key is applied to encrypt and decrypt the data. The advantages of the symmetric key cryptography are consuming less power with high speed. Moreover, it takes any one mode from the modes like stream ciphers and the block ciphers. The block cipher divides the whole data into small bits. It is faster than Asymmetric key cryptography. The asymmetric key cryptography method applies two different keys such as private and public keys for performing encryption and decryption process. Here, every user's having their own private key and public key. If the user (sender) sends the original data as encrypted data (cipher text) to any one user (receiver) then, the receiver is received the data and decrypt it as original text by using their own public key. The key exchange process is simple but the encryption and decryption processes are difficult and take more time. For example, the available public key algorithms such as RSA, Elliptic Curve Cryptography and Diffie-Hellman algorithms are useful for exchanging the keys.

In this work, a new secured storage algorithm is proposed for storing the data effectively by incorporating the newly proposed authentication, authorization, key management algorithms. In this work, Baye's theorem and the matrix translation are used for performing effective encryption, decryption and key management processes. This paper introduce a new Baye's theorem and Matrix translation based secured data storage method to store the cloud user's data securely in effective manner in cloud. Moreover, a new Baye's theorem-based authentication scheme to access the encrypted data from the cloud database. The proposed secured storage method incorporates an encryption method called Elliptic Curve Cryptography and also applies the matrix translation method for performing encryption process effectively. In addition, the matrix transposition method is applied for performing decryption process over the encrypted text. This work applies base theorem for generating keys for the cloud users to access the encrypted data that are taken from cloud server. The experiments have been carried out to evaluate the performance of the proposed secured data storage and retrieval model and it is proved the efficiency and effectiveness with respect to high security level than the available methods. Rest of the paper is organized as below: Section 2 described in detail about the related works on cryptography, secured data communications, cloud computing and networks. The merits and demerits of the works are discussed and also highlights the contributions for overcoming the dis advantages. Section 3 explains the overall system architecture of the proposed secured storage model. Section 4 discusses about the newly proposed algorithms along with the working flow. Section 5 demonstrated that the performance of the proposed model and the comparative analysis. Section 6 concludes the proposed model with future works.

2 Literature Survey

The various works have been done in the direction of cryptography, encryption, decryption, matrix-based encryption method, cloud storage and security and secured data communications by the different researchers in the past [5-6, 11-13, 17, 19-20, 25, 27-33, 39-40]. Among them, Wang et al [26] developed an attribute-based encryption method which works based on hierarchical manner which combines the hierarchical identity-based encryption and cipher-text policy and attribute aware encryption method that is useful for providing security. Peng, Zhao, Xie, Dai, Gao and Chen [28] provided an extensive result analysis that covers the cloud storage which cryptography methods have been applied for the effective design. Finally, they have declared that a best cryptographic method. Zhang, Xu, Xiang and Huang [36] developed a novel matrix-based pair-wise key development method.

Huang, Ma, Yang, Fu and Niu [29] developed a digital rights and cryptographic algorithms incorporated privacy preserved method to share the data. Koo, Hur and Yoon [30] developed a new data retrieval model that works based on attribute aware encryption for secured storage and ensured the privacy

preservation. The newly developed method is suitable for storing the huge amount of data and it supplies articulacy access and searching process with security. Moreover, it ensures the data security during the data retrieval process by using their method. Fu, Huang, Ma and Yang [31] developed a novel encryption technique with the incorporation of privacy preservation which is able to reduce the computational overhead of the decryption process, and also safeguards the privacy in data access as ciphertext and the features of cloud users. Liu, Wang and Wu [32] developed a time aware encryption method to access the data by the cloud users in a specific time duration.

Boomija and Raja [8] developed a secured data sharing key encryption method for preventing the illegal data outflow. Cui, Liu and Wang [14] discussed the practical issues that are not concentrated by the previous researchers. They have proposed a new key aggregation-based encryption method that instantiate the concept in which the owner of the data requires for sharing the keys to the various documents Finally, they have proved that their method is efficient than the existing systems. Yahyaoui and Kettani [9] aimed to develop a homomorphic encryption scheme which incorporates a noise free mathematical model for protecting the large volume of data in cloud. Jiang and Guo [10] developed a new dynamic data sharing method that is developed with the consideration of the conditional proxy re-encryption technique. Finally, they have illustrated that their method feasibility and also compared with existing method in this direction and proved as better. Pérez, Pérez and Gomez [15] developed a new access control policy which is created based on the roles and responsibility. They have proved as better than other models.

More, Chandugade, Rafiq and Pise [7] designed a security framework for protecting the delicate data. Their framework combines the ABE and the byte rotation encryption method to provide the protectivity, integrity and data exchange performance between two peers. Moreover, the data exchange is ensured the data visibility, consistency and security. Li, Shen, He, Gu, Xu and Xu [16] developed a new data sharing method which is a lightweight for the mobile cloud. Finally, their method reduces the cost overhead while performing the data sharing process in cloud. Zhang, Tian, Zhang, Yu and Li [34] developed a new matrix-based encryption and decryption method which applies the matrix transformation continuously. Their method provides the confidentiality by concealing the local data of the entries in the input. They have reduced the time overhead on client. Karame, Soriente, Lichota and Capkun [18] developed a new method which assured the confidentiality of the data even the encryption key is leaked. They have evaluated their method and also suggested that Bastion is a suitable to integrate the existing methodologies and proved that it takes less than 5% of overhead.

Aliev and Kim [35] developed a new authentication scheme with conditionally and matrix-based privacy preservation that is suitable for identifying the vehicle in the networks. Moreover, their scheme is achieved better authentication along with privacy dynamically. Ma, Zhang, Yang, Song, He and Xiao [21] developed a new access control incorporated data sharing method that is capable of handling electronic medical records effectively. They have proved as an efficient, practical and economical. Zhang, Cui and Mu [22] proposed a new privacy preserved attribute-based encryption method for verifying the authority verification. The keys are fixed size in their work and also achieved the selective security and the computational results are confirmed the advantages of their method. Manzoor, Braeken, Kanhere, Ylianttila and Liyanage [23] developed a new data sharing method which incorporates the blockchain technology for sharing the IoT data. Govindarajulu and Suresh [24] developed a privacy preserved model to protect the cloud users search patterns and also applied a probabilistic phrase recognition method. They have shown the efficiency of their model with better overheads by applying multi-keyword search patterns.

3 System Architecture

The overall architecture of the proposed model is shown in Figure 1 which contains ten important components such as Cloud Database, Cloud Service Provider (CSP), Key Generation Module, Encryption Module, Decryption Module, Decision Manager, User Interface Module, Rule Manager, Knowledge Base and Cloud User.

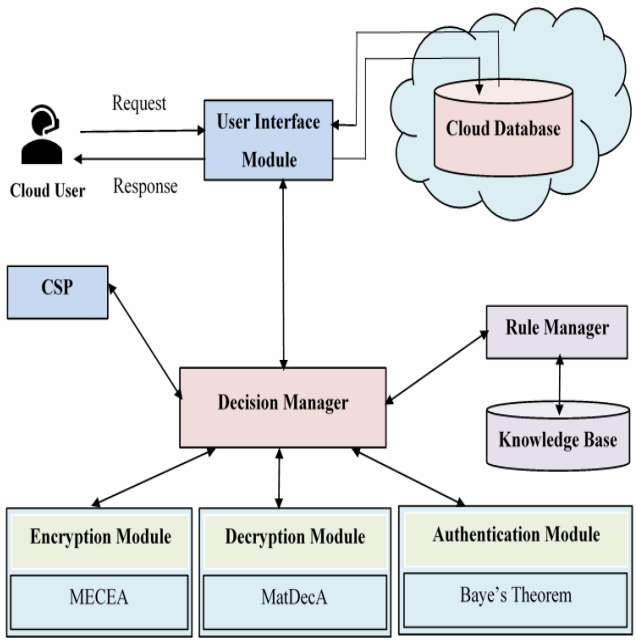

Figure 1. System architecture

Cloud User: The cloud user is sent the request to the CSP for storing and retrieving their data through user

interface module and the decision manager.

Cloud Database: The cloud database is capable of accommodating the volume of data. The stored data can be received by the cloud user through the decision manager.

User Interface Module: The user interface module is act as an intermediate component between the cloud user and the cloud database. Moreover, it also acts as a mediator between the cloud user and the decision manager.

CSP: The CSP is helpful for providing the necessary data from the cloud database securely through decision manager. The decision manager applies the three security modules such as Encryption module, decryption module and authentication module.

Decision Manager: The decision manager has overall control of the proposed system architecture. It handles the important components of this model such as encryption module, decryption module and authentication module. All the cloud user's requests will be sent to the CSP through this decision manager. The decision manager takes decision on various activities of the proposed model. The necessary rules also can be retrieved through rule manager from knowledge base which has all the necessary rules and facts.

Rule Manager: The rule manager manages the rules that are newly generated in this work. The necessary rules can be taken from knowledge base and send it to the respective modules for performing encryption and decryption and authentication processes.

Knowledge Base: The knowledge base stores the volume of data in the form of facts and rules. The necessary details are stored in the knowledge base which is useful performing the authentication, encryption and decryption processes effectively.

Encryption Module: The encryption module applies a newly proposed encryption algorithm called Matrix and Elliptic Curve Cryptography based Encryption Algorithm (MECEA) for performing effective encryption process in this work. Here, the original input text will be converted cipher text.

Decryption Module: The decryption module uses the newly developed decryption algorithm called MatDecA for decrypting the data. Here, the ciphertext will be converted into the plain text or original text. The keys were used for performing the decryption process with the help of the decryption module.

Authentication Module: The authentication module is responsible for generating new keys for providing the secret keys to the cloud users for accessing data in original form. The secret keys are helpful for converting the plain text to ciphertext and the cipher text to plain text. The secret keys are applied for performing encryption and decryption process and also ensured the data security in the cloud database.

4 Proposed Work

This section is described in detail about the proposed privacy preserving system for performing effective secured storage in cloud. This work proposes a novel secured data storage mechanism along with effective authentication scheme for maintaining the data in cloud. In the proposed model, the authentication of the cloud users is verified and validated by exchanging a key for the authorized cloud users. Here, the CSP is providing the accessibility only for authorized users to access the cloud data from the cloud databases. Moreover, they unable to access others data in the public cloud environment by applying their own keys and login details. The proposed model consists of three different algorithms such as Matrix Translation and ECC based Encryption Algorithm (MECEA), Matrix Transpose based Decryption Algorithm (MTDA) and the Bayes Theorem based Digital Signature Algorithm (BTDSA) for performing effective encryption, decryption and authentication process in cloud. This section is discussed about the background information about the Matrix operations, ECC, Bayes Theorem and the proposed algorithms along with mathematical proof.

4.1 Matrix Operations

The matrix operations are matrix translation and matrix transpose. These matrix operations are helpful for performing encryption process and the decryption processes in this work. This subsection is explained the matrix translation, matrix transpose and how these are useful for performing effective encryption and decryption processes.

4.1.1 Circular Matrix

Generally, the circular or cyclic matrix is the square matrix. And the elements of each row rotate one element to the right compared to the elements of the preceding row. The contribution of the cyclic matrix in cryptographic algorithm is highly contributing to increasing the level of security. For example, an $n \times n$ circular or cyclic matrix C,

$$C = \begin{vmatrix} C_0 & C_{n-1} & \cdots & C_2 & C_1 \\ C_1 & C_0 & C_{n-1} & \cdots & C_2 \\ \vdots & C_1 & C_0 & C_{n-1} & \vdots \\ C_{n-2} & \cdots & \cdots & C_0 & C_{n-1} \\ C_{n-1} & C_{n-2} & \cdots & C_1 & C_0 \end{vmatrix}$$

4.1.2 Matrix Transpose

Matrix Transpose means that the diagonal should remain the same and in the given matrix the upper part of the diagonal is shifted to the lower part of the diagonal and the lower part of the diagonal to the upper part of the diagonal in a specific way. That the way is, the columns are rearranged as the row or the rows are

rearranged as the columns. Set the numbers in matrix cyclic format is a secure method and application of the matrix transpose method is to increase its level of the security.

4.2 Elliptic Curve Cryptography

The term "Elliptic" is not meant that the equations are ellipses. Here, the common structure of the elliptic curve formula is given in equation(1).

$$y^2 = x^2 + ax + b \quad \textbf{(1)}$$

where 'a' and 'b' indicate the real numbers. Let consider 'a' holds the value of 2 and 'b' holds the value of 1. The curve which is generated by the standard Elliptic Curve Equation is shown in Figure 2.

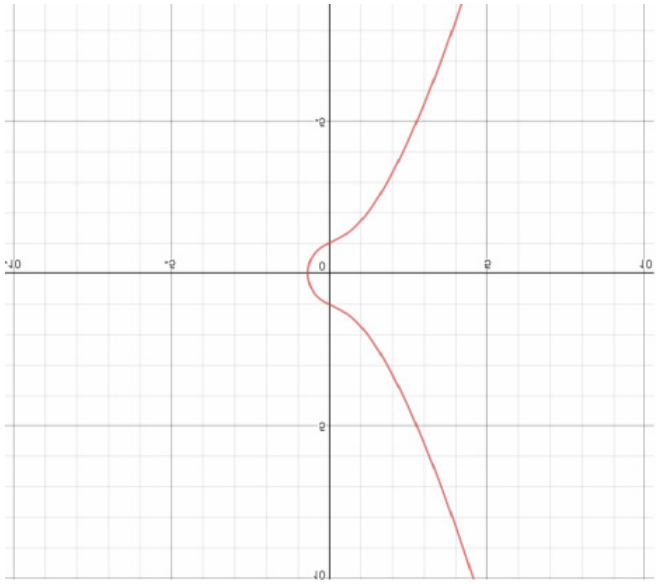

Figure 2. Elliptic curve

This elliptic curve is useful for performing the key generation process by using any point randomly which is available on the elliptic curve.

4.3 Baye's Theorem

Bayes' theorem is a mathematical formula to determine the conditional probability. The conditional probability produces the expected outcome according to the past experience or outcomes. It provides the prediction result or the possibilities as an extra knowledge or hint. Generally, it permits us to change the prediction result by considering new data and it is applied in various applications including finance for predicting the risk level. Formulae for the bayes theorem is given below:

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)} = \frac{P(A) \cdot P(B \mid A)}{P(B)} \quad \textbf{(2)}$$

Where, $P(A)$ indicates the probability of occurring A, $P(B)$ represents the probability of occurring B, $P(A|B)$ indicates that the probability of A given B, $P(B|A)$ represents the probability of B given A and the $A \cap B$ indicates that the probability of the occurrence of A and B. In this bayes theorem is applied in this work for predicting the points in the Elliptic Curve to identify the key which is useful for performing encryption and decryption processes on cloud data.

4.4 Encryption

This subsection is explained that the proposed encryption process which is done by applying the proposed encryption algorithm called Matrix Translation and Elliptic Curve based Encryption Algorithm (MECEA). The cloud data is considered for performing encryption process by following the below steps.

Matrix Translation and Elliptic Curve Cryptography Based Encryption Algorithm (MECEA)
Input: Input Data/Text (Plaintext)
Output: Encrypted form of Data/Text (Ciphertext)

Step 1: Read the text and it is divided into string and stored in 'T_i'.

Step 2: Calculate the ASCII value for the input text (string) and convert it into the 4-bit value of the given string and stored it in A_v and B_v, respectively.

Step 3: Compute the value of R using the formula, R = (ASCII) mod(n) where n is the n x n matrix.

Step 4: Create the $n \times n$ cyclic matrix A using the value of B_v.

Step 5: Compute A^T from the matrix A.

Step 6: Choose the R^{th} column and assign the new value of the given string. The newly generated ASCII value is stored in the T_n.

Step 7: Compute the curve equation with the values of 'u_i' and 'k_i', the Generated Elliptic Curve equation is $y^2 = x^3 + ax + b$ where $a = u_i$ and $b = k_i$.

Step 8: Generate the points on the Elliptic Curve.

Step 9: Choose random point's k and d from the generated points on the curve as secret keys.

Step 10: Compute the Q value using the formula given in equation (3)

$$Q = d \times P \quad \textbf{(3)}$$

Where, P is chosen from the generated points on the Elliptic Curve.

Step 11: Compute C_1 and C_2 values using the formulae given in the equation (4) and (5)

$$C_1 = k \times P \quad \textbf{(4)}$$

$$C_2 = T_n + (k \times Q) \quad \textbf{(5)}$$

Step 12: The encrypted text C_1, C_2 and d are sent to the cloud user as Ciphertext.

In this encryption algorithm, the original text is given as input and it will be converted into an unknown format of text which is able to understood by

the authorized users who have rights to access the data with the help of their own secret key.

4.5 Decryption

This subsection is explained that the proposed decryption process that is done by applying the proposed decryption algorithm called Matrix Transpose based Decryption Algorithm (MTDA). The cloud data is considered for performing decryption process by following the below steps.

Matrix Transpose Based Decryption Algorithm (MTDA)
Input: Ciphertext
Output: Original Text
Step 1: Compute the value of T_d using the formula of $T_d = C_2 - d \times C_1$.
Step 2: Choose any point on T_d and stored it in B_d.
Step 3: Create the $n \times n$ cyclic matrix B using the value of B_d.
Step 4: Compute the transpose of matrix B.
  a. Choose R^{th} row as the matrix B^T and stored in the T_d which is the *ASCII* value of the string.
  b. The transpose of a Matrix is a mechanism which twists a matrix over its diagonal. That means, it swapped the row to column or column to row of the matrix by making another new matrix.
Step 5: Convert *ASCII* value T_d into Original String 'S' and stored it in O_t.
Step 6: Decrypted text O_t display to the user.

The decryption process is able to produce the plain text from any cipher text which is provided as a result of the encryption algorithm.

4.6 Authentication

This subsection is explained that the authentication process of this proposed model. In this work, the authentication process is done by applying the newly proposed algorithm called Baye's Theorem based Digital Signature Algorithm (BTDSA) which is used to authenticate the cloud users. This authentication process is very useful and important for accessing the cloud data. Authentication process is necessary even the cloud users need to access their own data and their relevant information. The authentication process is done in this work as follows: First, choose two prime numbers p and q with the condition of $p > q$. The p-value will determine the size of the multiplicative group Zp^*. The q-value is considered as a threshold value in the process. The key server reads the user details while the user sends the request to the Key Server. That is, the key server reads the details of the user code and their position of the request. Then the user details to the Authentication module. In the Authentication module, a new proposed authentication algorithm which is based on the Bayes theorem processed. That is the method of authenticating the user by the probability between the user code in a closed group and the position of a request made by the user in a closed group. This method is called the Bayes theorem. The user's number is read from the closed group and stored in the u_i. The key server sends the user key to the user depending on the position of the user's request and saved it in 'k_i'. The key 'k_i' is chosen by the key server with the condition that 'k_i' value must be within the range of q.

Baye's Theorem Based Digital Signature Algorithm (BTDSA)
Input: Cloud User ID with Key
Output:
Step 1: Read the Cloud User details (Cloud User ID)
Step 2: User details stored in 'u_i'
Step 3: The Key Server generate the key 'k_i' based on the user request
Step 4: Compute the weight using the formula given in equation (6).

$$w_i = u_i + k_i \tag{6}$$

Signature:
1. Bayes Theorem formula, $P(u_i)$ = P(k_i) = Output Result / count of user and key in a pair (i.e) $P(u_i) = P(k_i) = 1 / 2$, where 1 is the required output and the value 2 is generated by the pair of user and key.
2. Compute the value of $P(A|u_i)$ and $P(A|k_i)$ using the formula given in equation (7) and (8).

$$P(A \mid u_i) = \frac{u_i}{q} \tag{7}$$

$$P(A \mid u_i) = \frac{k_i}{q} \tag{8}$$

3. Compute the value of v_i using the formulae given in equations (9)(10) and (11).

$$v_i = s + t \tag{9}$$

$$s = P(u_i)P(A \mid u_i) \tag{10}$$

$$s = P(k_i)P(A \mid k_i) \tag{11}$$

Verification:
1. Compute the value of y_i using the formula given in equation (12).

$$y_i = \frac{q}{P(k_i)} \tag{12}$$

2. Compute the value of r_i using the formula given in equation (13).

$$r_i = \frac{w_i}{y_i} \quad \textbf{(13)}$$

Compare: Compare the signature using the values of v_i and r_i.

$$v_i = r_i$$

4.7 Mathematical Proof

This section provides the mathematical proof for the processes of encryption, decryption and authentication in this work. First, the encryption process is demonstrated with the sample inputs.

4.7.1 Encryption

First, it reads the text as input and it is divided into string and also stored in '*T*' and also validate whether the input text is properly divided as various strings and ensure that all the contents are present as string or not. Then, calculates the ASCII value for the given input string and it converts into the 4-bit value of the given string and also stored it in A_v and B_v, respectively.

$A_v = 83$ || ASCII value of the string
$B_v = 0083$

Generate a $n \times n$ cyclic matrix A using the value of B_v.

$$A = \begin{vmatrix} 0 & 0 & 8 & 3 \\ 3 & 0 & 0 & 8 \\ 8 & 3 & 0 & 0 \\ 0 & 8 & 3 & 0 \end{vmatrix} \quad \| 4 \times 4 \text{ Cyclic Matrix}$$

Then, it calculates the R value using the formula, $R = (ASCII) \bmod (n)$ where n is the $n \times n$ matrix.

$R = 83 \bmod 4 = 3$ || 4 × 4 matrix
$R = 3$

After that, it calculates the value of R using the formula, $R = (ASCII) \bmod 8$

$R = 83 \bmod 4 = 3$
$R = 3$

Compute A^T value from the matrix A. Compute the new value of the given string using the matrix A, which is choosing the R^{th} column of the matrix A and stored in the T_n.

R^{th} column of the matrix is = 8003

Find the curve equation with the values of 'u_i' and 'k_i', the Generated Elliptic Curve equation is $y^2 = x^3 + ax + b \bmod p$ where $a = u_i$ and $b = k_i$.

$a = 7, b = 5$

Therefore, the Elliptic Curve Equation is $y^2 = x^3 + 7x + 5 \bmod 17$.

It creates the points on the Elliptic Curve as follows

(1, 8) (1, 9) (3, 6) (3, 11) (6, 5) (6, 12) (9, 7) (9, 10) (10, 2) (10, 15) (11, 6) (11, 11) (12, 7) (12, 10) (13, 7) (13, 10) (14, 5) (14, 12) (15, 0)

Choose the random point's k and d from the generated points on the curve as secret keys.

$k = (3, 6), d = (10, 2)$

Compute the Q value using the formula of $Q = d \times P$ where P is chosen from the generated points on the Elliptic Curve.

$P = (12, 7)$
$Q = d \times P = (10, 2) \times (12, 7) = (10 \times 12, 2 \times 7)$
$Q = (120, 14)$

Find the C_1 and C_2 values using the formula of $C_1 = k \times P$ and $C_2 = T_n + (k \times Q)$.

$C_1 = k \times P$
$= (3, 6) \times (12, 7)$
$C_1 = (36, 42)$
$C_2 = T_n + (k \times Q)$
$= 8003 + (3 \times 120, 6 \times 14)$
$= 8003 + (360, 84)$
$C_2 = (8363,8087)$

Finally, the encrypted text C_1, C_2 and d will be sent to the cloud user for the given input string or the available cloud data.

4.7.2 Decryption

This section is demonstrated that the working process of the proposed model. The decryption process is done in this work as follows: First, it calculates the value of T_d using the formula of $T_d = C_2 - d \times C_1$.

$T_d = C_2 - d \times C_1$
$= (8363,8087) - (10 \times 36, 2 \times 42)$
$= (8363,8087) - (360, 84)$
$= (8363 - 360,8087 - 84)$
$T_d = (8003,8003)$

Select any one point on T_d and stored it in B_d.

$T_d = (8003,8003)$
$B_d = 8003$

Create the $n \times n$ cyclic matrix B using the value of B_d.

$$B = \begin{vmatrix} 8 & 0 & 0 & 3 \\ 3 & 8 & 0 & 0 \\ 0 & 3 & 8 & 0 \\ 0 & 0 & 3 & 8 \end{vmatrix} \quad \| 4 \times 4 \text{ Cyclic Matrix}$$

Generate the transpose of matrix for the matrix B as below.

$$B^T = \begin{vmatrix} 8 & 3 & 0 & 0 \\ 0 & 8 & 3 & 0 \\ 0 & 0 & 8 & 3 \\ 3 & 0 & 0 & 8 \end{vmatrix} \quad \| 4 \times 4 \text{ Cyclic Matrix}$$

Then, it selects R^{th} row as the matrix B^T and it is also stored in the T_d which is the ASCII value of the string. Then, the value is converted from *ASCII* value of T_d into the original string S and it stored it in O_t. Afterwards, decrypted the original text O_t and display to the cloud user.

4.7.3 Authentication

This subsection is demonstrated that the authentication process with a sample input. First, selects any two prime numbers p and q with the condition of $p > q$.

$$p = 17, q = 13 \quad || p > q$$

First, read the cloud user id or employee id or code. For example, the cloud user id is 7. The cloud user id is stored in 'u_i'. Now, the variable u_i holds the value of 7. The key server generates the key 'k_i' based on the cloud user request. Let assume that k_i holds 5. Find the value of w_i by adding the values of u_i and k_i.

$$w_i = 7 + 5 = 12$$
$$w_i = 12$$

The signature creation process is done within this authentication process. Here, the existing Bayes Theorem is applied for finding the probability of the u_i and k_i by using the formula: P(u_i) = P(k_i) = Output Result / count of user and key in a pair (i.e) and P(u_i) = P(k_i) = 1 / 2, where 1 is the required output and The value 2 is generated by the pair of user and key.

Calculates the value of P(A|u_i) and P(A|k_i) using the formula of

$$P(A|u_i) = u_i / q \text{ and } P(A|k_i) = k_i / q$$
$$P(A|u_i) = u_i / q = 7 / 13$$
$$P(A|k_i) = k_i / q = 5 / 13$$

Find the value of V_i, $V_i = s + t$ where s = $P(u_i)$ $P(A|u_i)$and $t = P(k_i)$ $P(A|k_i)$.

$$s = P(u_i)\ P(A|u_i)$$
$$= [1 / 2] \times [7 / 13]$$
$$s = 7 / 26$$
$$t = P(k_i)\ P(A|k_i)$$
$$= [1 / 2] \text{ x } [5 / 61]$$
$$= 5 / 26$$
$$V_i = s + t$$
$$= [7 / 26] + [5 / 26]$$
$$V_i = 12 / 26$$

The verification process is done by calculating the value of y_i and r_i. First, find the value of y_i as below:

$$y_i = q / P(k_i)$$
$$y_i = q / P(k_i)$$
$$= 13 / [1 / 2]$$
$$= 13 \times 2$$
$$y_i = 26$$

Then, computes the value of r_i using the formula $r_i = w_i / y_i$. Now, the w_i holds the value of 12 and the y_i holds the value of 26.

$$r_i = w_i / y_i$$
$$r_i = 12 / 26$$

Now, we have the values of v_i and r_i. Finally, these two values can be compared and finalized the authentication process if it is equal.

5 Results and Discussion

This section demonstrated that the performance of the proposed model based on the standard evaluation metrics. The proposed model has been implemented by using Java programming, Net Beans and CloudSim. The performance of the proposed model is measured by conducting various experiments with respect to the different performance metrics such as key generation time, encryption time, decryption time, execution time and the overall computational time.

5.1 Evaluation Metrics

The standard evaluation metrics including key generation time, encryption time, decryption time, execution time and the overall computational time are discussed in this subsection with formulas.

Key Generation Time: It is the total time taken for generating key for the particular amount of data and it is calculated by using the formula given in equation (14):

$$KGT = (DTT + EXT) \quad \textbf{(14)}$$

Where, KGT means that the time taken for generating the keys, DTT indicates that the time taken for transferring the data and EXT represents the execution time.

Encryption Time: It is the time taken by the data owner for encrypting the plain text to ciphertext. In general, the encryption time of any algorithm is indicated that in terms of milliseconds and also computed by applying the equation (15).

$$ET = ENT - STT \quad \textbf{(15)}$$

Where, ET means that the encryption time, ENT represents the ending time and the STT indicated the starting time.

Decryption Time: It is a time taken by the data user for decrypting the input data which expresses in terms of milliseconds and it is also computed by applying the formula given in equation (16).

$$DT = ENT - STT \quad \textbf{(16)}$$

Where, DT means that the decryption time, ending time/Completion time is represented as ENT and the starting time is represented as STT.

5.2 Experimental Results

The various experiments have been carried out in

this work for proving the efficiency and effectiveness of the proposed model in terms of the evaluation metrics such as encryption time, decryption time, key generation time. First, Figure 3 demonstrates that the key generation time analysis for the proposed secured storage model. Here, the different number of cloud users such as 100, 200, 300, 400 and 500 cloud users were considered in five different experiments such as E1, E2, E3, E4 and E5 in this work.

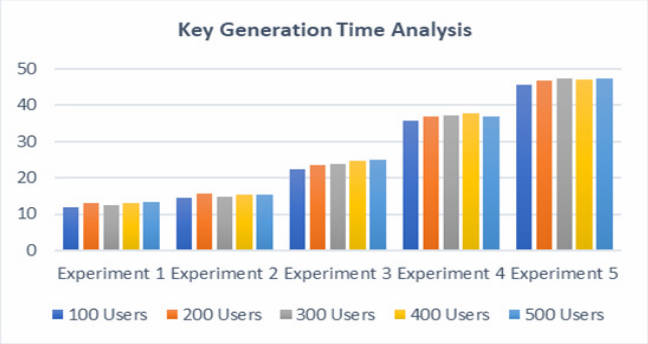

Figure 3. Key generation time analysis

From Figure 3, it is proved that the efficiency of the proposed model in terms of key generation time. Here, the key generation time is gradually increasing the key generation time while increasing the number of cloud users in the cloud. The reason for the performance enhancement is the introduction of the bayes theorem for generating keys and also verify them in the process of authentication process.

The encryption time analysis of the proposed model is shown in Table 1 which consists of five different experiments. In this analysis, the various sizes of records or files are considered for the five different experiments as input data in cloud. The various sizes of input files with 100 kb, 200kb, 300 kb, 400kb and 500 kb are considered to evaluate the proposed secured storage and data communication model effectively.

Table 1. Encryption time analysis

Exp./ File Size (Kb's)	Encryption Time (in Seconds)				
	100	200	300	400	500
E1	10	21.6	34.5	45.3	55
E2	11	22	45.3	44.9	55.6
E3	10.5	22.5	35.6	45.6	54.9
E4	11.2	22.3	35.4	45.4	55.3
E5	11.3	21.9	35.8	45.2	55.8

From Table 1, it can be seen that the performance of the proposed model is stable in terms of the seconds. The five experiments are taken almost equal amount time for handling the specific size of input file. Even though, the encryption time is increasing gradually while increasing the input file size due to the use of matrix and Baye's theorem.

The encryption time analysis of the proposed model is shown in Table 2 which consists of five different experiments. In this analysis, the various sizes of records or files are considered for the five different experiments as input data in cloud. The various sizes of input files with 100 kb, 200kb, 300 kb, 400kb and 500 kb are considered to evaluate the proposed secured storage and data communication model effectively.

Table 2. Decryption time analysis

Exp. Exp./ File Size (Kb's)	Decryption Time (in Seconds)				
	100	200	300	400	500
E1	9.5	20.9	33.3	44.2	53.4
E2	10.4	21.6	34.4	43.8	54.1
E3	10.6	21.4	34.6	44.8	53.5
E4	10.3	21.4	34.2	44.5	53.9
E5	10.1	20.8	34.9	44.1	54.2

From Table 2, it can be seen that the performance of the proposed model is stable in terms of the seconds. The five experiments are taken almost equal amount time for handling the specific size of input file. Even though, the encryption time is increasing gradually while increasing the input file size due to the use of matrix and theorem.

The comparative analysis between the proposed secured storage model and the existing systems in terms of execution time. For this purpose, the execution time analysis is done in this work by conducting various experiments and also taken average performance of the different experiments and considered as a final result of the work. In this computational time analysis, the equal number of cloud users as 20 along with same size of input data as10 GB. Moreover, the existing works in this direction such as DSVS, PP-ESAP, DRDA, ECDH-ECC and EC(DH)^2 [38].

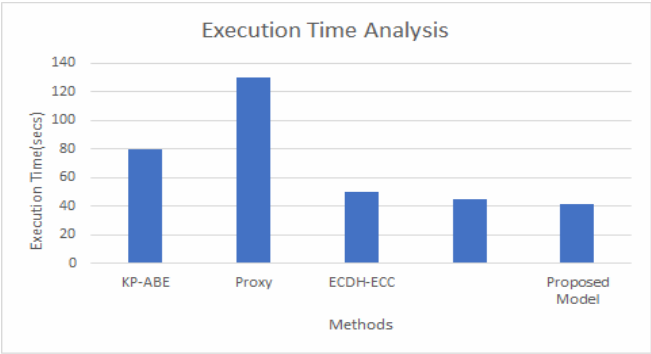

Figure 4. Comparative analysis w.r.t execution time

From Figure 4, it is observed that the proposed model is performed well than the existing works such as KP-ABE, Proxy, ECDH-ECC and EC(DH)^2. The reason for the enhancement in the proposed model is the application of circular matrix in encryption process, matrix transpose in decryption process and the Baye's theorem in authentication process. Due to the use of all these techniques, the performance of the proposed

algorithm is achieved better as less execution time even uses the same number of cloud users with same size of data. Figure 5 shows the security level analysis between the proposed model and the existing works such as KP-ABE, EC(DH)^2 and CRT based secured storage mechanism [37].

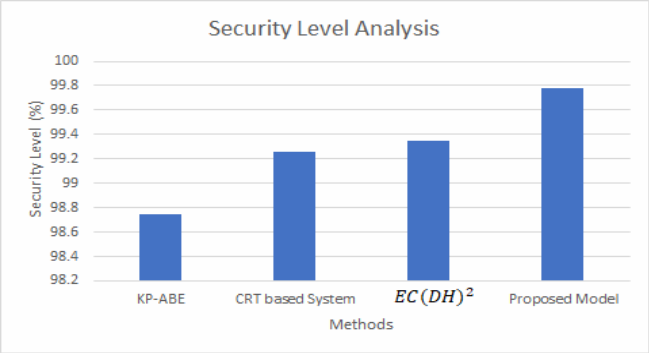

Figure 5. Security level analysis

The proposed model is achieved better security level due to the use of matrix and Baye's theorem.

6 Conclusion and Future Work

This paper introduces a new Baye's theorem and Matrix translation based secured data storage method to store the cloud user's data securely in effective manner in cloud. Moreover, a new Baye's theorem-based authentication scheme to access the encrypted data from the cloud database. The proposed secured storage method incorporates an encryption method called Elliptic Curve Cryptography and also applies the matrix translation method for performing encryption process effectively. In addition, the matrix transposition method is applied for performing decryption process over the encrypted text. This work applies base theorem for generating keys for the cloud users to access the encrypted data that are taken from cloud server. The experiments have been carried out to evaluate the performance of the proposed secured data storage and retrieval model and it is proved the efficiency and effectiveness with respect to high security level than the available methods. Future work in this direction is the introduction of effective encryption, decryption and key generation techniques for enhancing the cloud performance in terms of efficiency.

References

[1] A. J. Paul, P. Mythili, K. Jacob, Matrix based cryptographic procedure for efficient image encryption, *2011 IEEE Recent Advances in Intelligent Computational Systems*, Trivandrum, India, 2011, pp. 173-177.

[2] E. B. P. Manurung, O. S. Sitompul, Suherman, Applying transpose matrix on advanced encryption standard (AES) for database content, *2nd International Conference on Computing and Applied Informatics*, Medan, Indonesia, 2017, pp. 1-6.

[3] D. Rathi, P. Astya, Extended Hill Cipher Decryption by Using Transposed Interweaved Shifting, *International Journal of Computer Science and Information Technologies*, Vol. 5, No. 2, pp. 1147-1151, March-April, 2014.

[4] U. Thirupalu, E. K. Reddy, A New Cryptosystem for Ciphers using Transposition Techniques, *International Journal of Engineering Research & Technology*, Vol. 8, No. 4, pp. 402-406, April, 2019.

[5] V. Thakor, P. Ghosh, P. Bhathawala, An Approach of Hybrid Transposition method based on ASCII value in Cryptography, *International Journal of Advanced Computational Engineering and Networking*, Vol. 5, No. 7, pp. 104-107, July, 2017.

[6] K. R. Devi, G. N. Harshini, Analysis and Comparison of Substitution and Transposition Cipher, *International Journal of Research and Analytical Reviews*, Vol. 6, No. 2, pp. 549-555, April-June, 2019.

[7] P. More, S. Chandugade, S. M. S. Rafiq, P. Pise, Hybrid Encryption Techniques for Secure Sharing of a Sensitive Data for Banking Systems Over Cloud, *2018 International Conference On Advances in Communication and Computing Technology (ICACCT)*, Sangamner, India, 2018, pp. 93-96.

[8] M. D. Boomija, S. V. K. Raja, Secure data sharing through additive similarity based ElGamal like encryption, *2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, Chennai, India, 2016, pp. 652-655.

[9] A. E. Yahyaoui, M. D. E. C. E. Kettani, A verifiable fully homomorphic encryption scheme to secure big data in cloud computing, *2017 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, Rabat, Morocco, 2017, pp. 1-5.

[10] L. Jiang, D. Guo, Dynamic Encrypted Data Sharing Scheme Based on Conditional Proxy Broadcast Re-Encryption for Cloud Storage, *IEEE Access*, Vol. 5, pp. 13336-13345, July, 2017.

[11] A. Awad, A. Matthews, Y. Qiao, B. Lee, Chaotic Searchable Encryption for Mobile Cloud Storage, *IEEE Transactions on Cloud Computing*, Vol. 6, No. 2, pp. 440-452, April-June, 2018.

[12] K. Lee, Comments on "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption", *IEEE Transactions on Cloud Computing*, Vol. 8, No. 4, pp. 1299-1300, October-December, 2020.

[13] Q. Huang, W. Yue, Y. He, Y. Yang, Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing, *IEEE Access*, Vol. 6, pp. 36584-36594, July, 2018.

[14] B. Cui, Z. Liu, L. Wang, Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage, *IEEE Transactions on Computers*, Vol. 65, No. 8, pp. 2374-2385, August, 2016.

[15] J. M. M. Pérez, G. M. Pérez, A. F. S. Gomez, SecRBAC: Secure data in the Clouds, *IEEE Transactions on Services Computing*, Vol. 10, No. 5, pp. 726-740, September-October,

2017.

[16] R. Li, C. Shen, H. He, X. Gu, Z. Xu, C. Xu, A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing, *IEEE Transactions on Cloud Computing*, Vol. 6, No. 2, pp. 344-357, April-June, 2018.

[17] P. K. Tysowski, M. A. Hasan, Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds, *IEEE Transactions on Cloud Computing*, Vol. 1, No. 2, pp. 172-186, July-December, 2013.

[18] G. O. Karame, C. Soriente, K. Lichota, S. Capkun, Securing Cloud Data Under Key Exposure, *IEEE Transactions on Cloud Computing*, Vol. 7, No. 3, pp. 838-849, July-September, 2019.

[19] Z. Zhu, R. Jiang, A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 27, No. 1, pp. 40-50, January, 2016.

[20] C. Zuo, J. Shao, J. K. Liu, G. Wei, Y. Ling, Fine-Grained Two-Factor Protection Mechanism for Data Sharing in Cloud Storage, *IEEE Transactions on Information Forensics and Security*, Vol. 13, No. 1, pp. 186-196, January, 2018.

[21] H. Ma, R. Zhang, G. Yang, Z. Song, K. He, Y. Xiao, Efficient Fine-Grained Data Sharing Mechanism for Electronic Medical Record Systems with Mobile Devices, *IEEE Transactions on Dependable and Secure Computing*, Vol. 17, No. 5, pp. 1026-1038, September-October, 2020.

[22] L. Zhang, Y. Cui, Y. Mu, Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing, *IEEE Systems Journal*, Vol. 14, No. 1, pp. 387-397, March, 2020.

[23] A. Manzoor, A. Braeken, S. S. Kanhere, M. Ylianttila, M. Liyanage, Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain, *Journal of Network and Computer Applications*, Vol. 176, Article No. 102917, November, 2021.

[24] M. Govindarajalu, S. R. Suresh, Intelligent secure phrase search of encrypted data in cloud based IoT, *Materials Today: Proceedings*, pp. 1-3, January, 2021.

[25] Z. Ali, S. A. Chaudhry, K. Mahmood, S. Garg, Z. Lv, Y. B. Zikria, A clogging resistant secure authentication scheme for fog computing services, *Computer Networks*, Vol. 185, Article No. 107731, February, 2021.

[26] G. Wang, Q. Liu, J. Wu, M. Guo, Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers, *Computers & Security*, Vol. 30, No. 5, pp. 320-331, July, 2011.

[27] Q. Liu, G. Wang, J. Wu, Secure and privacy preserving keyword searching for cloud storage services, *Journal of Network and Computer Applications*, Vol. 35, No. 3, pp. 927-933, May, 2012.

[28] Y. Peng, W. Zhao, F. Xie, Z. H. Dai, Y. Gao, D. Chen, Secure cloud storage based on cryptographic techniques, *The Journal of China Universities of Posts and Telecommunications*, Vol. 19, No. 2, pp. 182-189, October, 2012.

[29] Q. Huang, Z. Ma, Y. Yang, J. Fu, X. Niu, Secure and privacy-preserving DRM scheme using homomorphic encryption in cloud computing, *The Journal of China Universities of Posts and Telecommunications*, Vol. 20, No. 6, pp. 88-95, December, 2013.

[30] D. Koo, J. Hur, H. Yoon, Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage, *Computers & Electrical Engineering*, Vol. 39, No. 1, pp. 34-46, January, 2013.

[31] J. Fu, Q. Huang, Z. Ma, Y. Yang, Secure personal data sharing in cloud computing using attribute-based broadcast encryption, *The Journal of China Universities of Posts and Telecommunications*, Vol. 21, No. 6, pp. 45-51, December, 2014.

[32] Q. Liu, G. Wang, J. Wu, Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, *Information Sciences*, Vol. 258, pp. 355-370, February, 2014.

[33] M. Aliasgari, O. Simeone, J. Kliewer, Private and Secure Distributed Matrix Multiplication with Flexible Communication Load, *IEEE Transactions on Information Forensics and Security*, Vol. 15, pp. 2722-2734, 2020.

[34] S. Zhang, C. Tian, H. Zhang, J. Yu, F. Li, Practical and Secure Outsourcing Algorithms of Matrix Operations based on a Novel Matrix Encryption Method, *IEEE Access*, Vol. 7, pp. 53823-53838, April, 2019.

[35] H. Aliev, H. W. Kim, Matrix-Based Dynamic Authentication With Conditional Privacy-Preservation for Vehicular Network Security, *IEEE Access*, Vol. 8, pp. 200883-200896, November, 2020.

[36] Y. Zhang, L. Xu, Y. Xiang, X. Huang, A matrix-based pairwise key establishment scheme for Wireless Mesh Networks using Pre Deployment Knowledge, *IEEE Transactions on Emerging Topics in Computing*, Vol. 1, No. 2, pp. 331-340, December, 2013.

[37] B. P. Kavin, S. Ganapathy, A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications, *Computer Networks*, Vol. 151, pp. 181-190, March, 2019.

[38] B. P. Kavin, S. Ganapathy, EC(DH)2: an effective secured data storage mechanism for cloud based IoT applications using elliptic curve and Diffie-Hellman, *International Journal of Internet Technology and Secured Transactions*, Vol. 10, No. 5, pp. 601-617, May, 2020.

[39] S. Wu, C. Hsu, Z. Xia, J. Zhang, D. Wu, Symmetric-bivariate-polynomial-based Lightweight Authenticated Group Key Agreement for Industrial Internet of Things, *Journal of Internet Technology*, Vol. 21, No. 7, pp. 1969-1979, December, 2020.

[40] S. Khatoon, S. M. M. Rahman, R. Tso, M. F. Alhamid, An Efficient and Secure, ID-based Authenticated, Asymmetric Group Key Agreement Protocol for Ubiquitous Pay-TV Networks, *Journal of Internet Technology*, Vol. 21, No. 5, pp. 1387-1395, September, 2020.

Biographies

Nithisha J is working as an Assistant Professor in Department of Information Technology at Jeppiaar Engineering College, Chennai. She is doing part time research in Information & Communication Engineering, Anna University, Chennai. Her research areas of interest are Cloud Computing and Network Security.

Jesu Jayarin P is working as professor in Computer Science And Engineering, Jeppiaar Engineering College, Chennai, Tamil Nadu, India. He has received his Ph.D. Degree from Sathyabama University, Chennai, India. He has more than 16 years of teaching experience. He has published more than 50 papers. His research interests including Cloud Computing.