I. J. Computer Network and Information Security, **2022, 6, 76-88**
Published Online on December 8, 2022 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2022.06.06

Modified ECC for Secure Data Transfer in Multi-Tenant Cloud Computing

S. Udhaya Chandrika*
Bharathiar University, Coimbatore, Tamil Nadu
E-mail: udhayachandrika05@gmail.com
*Corresponding Author

T. Pramananda Perumal
Principal (Retd.)/ Presidency College /CSE/ Chennai, India, 600005

Received: 07 July 2021; Revised: 19 February 2022; Accepted: 27 May 2022; Published: 08 December 2022

Abstract: Cloud computing technologies comprise various kinds of significant desirable constrains such as security, liability, government surveillance, telecommunications capacity, anonymity and privacy. The usage of cipher text technology is considered as a desired technique for performing the process of encryption in order to solve the issue of granting security to the data that are shared in the cloud. Similarly, the architecture of multi-tenant in the cloud computing system grants benefits to both the service providers and end-users which shares a common cloud platform to multiple tenants (i.e.) users and suitable resources are also computed by implementing proposed architecture. Therefore in this research work, the concept of cipher text multi-tenant are integrated for providing enhanced security to the data shared in the cloud environment. Hence a Modified Elliptic Curve Cryptography (MECC) based on Diffee Hellman algorithm is proposed in this research paper which provides enhanced security using alternate key generation. The encryption, decryption, upload and download time are calculated and it is concluded that the algorithm that is proposed in this research paper consumes less time for all these measures when comparing with other existing algorithms. Characteristics like less memory, high operational performance, small sized keys and rapid key generation process, and effective resource savings enable the modified ECC to obtain high efficiency. The encryption time of the proposed MECC system was 51ms with the key length 4096 bits, whereas existing method had 92 ms as encryption time. Likewise With the key length of 4096 bits, the decryption time for the proposed model was 159 ms. Accordingly the proposed system has reduced cipher text key size of 836KB when compared with the existing AES, Blow Fish, and Two Fish. Additionally, the key generation time (35 s) also seems to be considerably reduced when compared with the existing methods. These statements reveal that the proposed system outshine the state of art methods in terms of key generation time, encryption and decryption time and computational complexity.

Index Terms: Cloud Computing, Cipher Text, Multi-tenant, Modified Elliptic Curve Cryptography (MECC), Encryption, and Decryption.

1. Introduction

Cloud computing technology is an emanate paradigm to meet research and business requirements in a smarter approach. Cloud storage offer several advantages like huge storage, fast access and data availability for data retrieval [1, 2]. For data retrieval by the end user, their corresponding attribute set must match the access tree values that has been embedded to access policy. For data decryption, these attribute set must satisfy the specified condition in the access policy [3, 4]. Each layer of cloud computing is found to highly responsible for specific services in which SaaS layer enable accession to desired software thereby avoids downloading to our system, IaaS controls networks, virtual machines etc., and PaaS offers facility to employ various applications or services with reduced cost and software governing difficulties [5, 6]. The users of cloud computing must encrypt the data before sharing their data to the cloud in order to provide proper security from leaking the data [7, 8]. The process of controlling the access is the first and vital step in providing the security for preventing the unauthorized accessing of the data that have been shared. Numerous services are provided to the clients by the CSP (i.e.) Cloud Service Provider which acts as the manager for various cloud servers. The cipher text is generated by the data owner which is also responsible for the encryption and uploading of the cipher text to the CSP. The required cipher text is decrypted and downloaded by the user from the CSP A separate hierarchical structure is present for the files that are shared (i.e.) the shared group of files are converted to a.

numerous hierarchical subdivision which are placed at various access levels. By utilizing an integrated access structure, the files that are placed in the same hierarchical structure are encrypted. Therefore, the time and cost required for the decryption and storage cost for the cipher text are reduced [9].

The information's that are shared in the computer systems are secured by the utilization of a powerful tool known as cryptography [10, 11]. Numerous cryptographic algorithms are utilized for granting required security to the data transferred to the bank, while using home banking by a browser n a computer. When an unauthorized person tries to access the computer, cryptographic hash functions are employed for protecting the password. Then SSL is employed for encrypting an email during the time of sending. Cryptography involves the procedure to encode the original message in a non-readable format. The above procedure is termed with the name of encryption. Then the original information is obtained by the authorized person who decodes the encrypted message in an appropriate manner. And this procedure is termed as decryption [12-14].

Every user of the cloud computing is referred with the name of tenant and the corresponding process of permitting the tenants is known as tenancy. Multi-tenancy is one such process that comprise of a separate architecture that serves multiple tenants through the functioning of a single software. [15] It is considered as one among the key features involved in the cloud computing. The shared data is not interacted to other tenants and a separate dedicated cloud service is provided to a single tenant in the traditional cloud architecture of single tenant [16]. But this approach does not grant much accessible cloud services and saving in terms of cost for the service provider. Whereas information's such as the database, infrastructure and applications etc. are shared in general to all the tenants of a cloud in the multi-tenant cloud computing technique. But this consist of limitations like the specific expectations of the tenants are not satisfied as they could not customize or modify the usage of cloud services. Elliptic Curve Diffie Hellman (ECDH) is a key exchange agreement that enable the data owner and data user for establishing a shared information (key) over insecure channel. ECDH multiplies the private key by the public key obtained from data owner for getting the shared secret information [17]. This secret information has been utilized for performing symmetric encryption. Out study has been motivated by the following advantages of ECDH: less memory, high operational performance, small sized keys and rapid key generation process, and effective resource savings.

1.1. Significance of the Study

Due to the processing of huge amount of data, it is highly necessary to ensure security. Meanwhile it is also necessary to reduce the computational complexity and time complexity. Hence this research work attempted to provide secure and reliable data transmission into the cloud through Modified ECC method. While dividing the private key into two (on the basics of size) and encrypt it separately means, we will get two private keys. That will be stored in the cloud. For each document encryption, the key will be stored in the cloud so that only we can reverse the process for the decryption. It makes the algorithm more Secure. By exchanging public keys for encrypting data, MECC encryption securely exchanges information over untrusted channels. It is the most secure encryption process because users are never required to reveal or share their private keys, if they got means they need two private Diffie Hellman encrypted keys to decrypt a single Private Key from the ECC. Thus, decreasing the chances of a cybercriminal discovering a user's private key during transmission. Then in the perspective of cloud service model, the multi-tenant technique is approached differently. To solve this limitation a Modified Elliptic Curve Cryptography (MECC) is proposed for securing information's shared to the multi-tenant cloud computing architecture with the help of the generating keys.

1.2. Problem Statement

Recent studies possess various challenges like computational complexity, key generation time extension, noise sensitivity, breaking huge clusters, difficulty during handling of different cluster size etc., thereby influencing the end data retrieval results. Further traditional Hierarchical clustering possess various complexities in the selection of merge and split points and handling of huge dataset followed by the presence of arbitrary decisions. This paper attempted to overcome these limitations with the proposed ECDH based cryptography and Pearson correlation coefficient based hierarchical clustering.

1.3. Objectives

The objectives involved in the research work is mentioned below:

- To perform effective cryptographic process with the modified ECC that reduced key size and high security thereby overcoming prevailing limitations like low operational performance, time and computational complexity.
- To reduce the encryption and decryption time with the fast performing capability of the proposed MECC that implies Diffie Hellman algorithm based modification.
- To increase the accuracy and to generate alternate keys for security improvement with the presented modified differ Hellman based modified model.
- To evaluate the performance of the proposed model in terms of performance metrics such as encryption and decryption time, and computational complexity
- To compare the effectiveness of the proposed model with other state of art models.

1.4. Paper Organization

The organization of the paper is described as follows. The literature part of different cloud computing techniques for data security is given in Section II. Section III labels the proposed methodology procedure of Modified Elliptic Curve Cryptography (MECC) and the flow diagram. The evaluation results of the proposed method is specified in section IV. Finally, the effectiveness of the proposed method is concluded in section V.

2. Related Works

The research works that discusses the similar concepts related to cloud computing, encryption and decryption then multi-tenant are reviewed in this related works section. These works are reviewed in detail along with their advantages and disadvantages.

2.1. Cloud Computing

A cloud computing adoption framework for multilayered has been framed by [18] security contains three major security such as firewall, identity management and encryption depend upon growth of enterprise file synchronization and share method. The advantage was that core technology provides better robustness multilayered security in cloud computing environment. The disadvantage was that cloud computing adoption framework does not acquire any false alarm within specific period of time. A penetration testing could be identified and blocked virus about 99.95 percentage. A complete cloud computing adoption could be blocked each structured query language injection and also delivers original data protection. Finally, a multilayered security such as volume, velocity and veracity of big data services could be performed in cloud. The present study attempted overcome the time complexity with the modified ECC method that utilize small sized key.

There exist several studies that explicated about the integration of cloud and IoT, such that [19] aimed to provide certain properties of cloud computing environment. The advantage was that an innovative Cloud IoT method was suggested to offer better knowledge between users. The disadvantage was that user required to prevent and solve detailed analysis of cloud computing issues within given time. To overcome drawback, original cloud and IoT technique could be established to adopt number of applications gaining momentum and also to update Cloud IoT parameters. The main objective was to represent different techniques acquired in cloud IoT applications from both proprietary and open-source projects employing the Cloud IoT paradigm. Finally, the open issues in cloud computing could be detected that play important part in setting future internet process. Similarly, the presented study also tried to overcome these time complexity issues. Mobile cloud computing was comprehensively explained by [20], where this study was developed to allow mobile users to obtain cloud computing benefits by utilizing an environmentally friendly method in an effective manner from meeting industrial demands. The advantage was that a dynamic energy-aware cloudlet-based mobile cloud computing model could be focused properly to resolve extra energy consumption at the time of wireless communications by utilizing dynamic cloudlets based model. The disadvantage was that wireless bandwidth and device capacity got limited like additional energy waste and latency delay if the mobile cloud computing got deployed. The main aim of this research was to resolve energy waste issues inside dynamic networking environment and deliver better theoretical supports. Finally, the proposed method in cloud computing could be delivered for estimation of research process in future. The presented work had less latency as well as less energy loss.

Moreover, to analyze the nDCs energy consumption, [21] recommended time based energy and flow based energy consumption models. These models were applied for shared and unshared network equipment. There are set of experiments and measurements were compared for the validation of these models. The number of determinations includes the system design factor and it allows nDCs to spend the less energy than its centralized counterpart. It includes the various types of access network for Nano servers and time utilization of nano servers. nDCs applications contains the factors of number of updates, number of downloads, and energy cost. The results proved the total energy consumption with mentioned factors. They showed the Nano servers in Fog computing which can complement the centralized data centers to help certain applications of IoT. The cloud computing landscape contains significant changes over last decade. [22] discussed the changing cloud infrastructure and the usage of infrastructure from various providers and decentralizing computing benefits were away from DCs. This result requires for different new computing architectures which will be offered by future cloud infrastructure. These architectures were expected to impact areas named data intensive computing, connecting people and devices and self-learning systems. At the end, they described the challenges that requires to get addressed for analyzing the potential of cloud systems in next generation.

Position figures and tables at the center of the page. Figure captions should be Left-Aligned below the figures; table captions should be Left-Aligned above. Avoid placing figures and tables before their first mention in the text. Use the abbreviation “Fig. 1,” even at the beginning of a sentence.

2.2. Encryption and Decryption

Moreover, because of the privacy concerns, the confidential data should be encrypted before it is uploaded to cloud. Over past years, various studies have suggested several encryption systems. Nevertheless, majority of the prevailing works focus only on secure searching by utilizing keyword, and also it retrieves only Boolean outcomes, which aren’t

adequate. In order to solve this issue, [23] designed a novel secured keyword search method on the basis of Bloom filter that improvises the usability by enabling ranking based on search results. Instead of retrieving every files, this method retrieves only the relevant files. Furthermore, BFs (Bloom filters) accelerates search process, which involves more keywords.

[24] elected ECC (Elliptic curve cryptography) for data encryption and tenant authentication because of its minimal key size. The suggested ECC based authorization method enables the authenticated persons in accessing confidential data. Also, it efficiently secures from diverse attacks. In order to develop a secured data encryption method, the study integrated nature inspired optimization method like MSA (Moth search algorithm) with ECC for selecting optimum and correct values of elliptic curve. Further, the recommended decryption and encryption technique integrates DNA encoding with ECC encryption method. From the experimental analysis, the outcomes of the study revealed that the average execution time of recommended method was 86.076 seconds for decryption and 83.153 for encryption. Additionally, the study stated that the presented method offers two layer security with significantly lesser storage as well as minimal key size.

There exist several encryption techniques for securing private data, however they have certain limitations such as increased decryption, encryption as well as key generation time. In order to solve these problems, [25] introduced an efficient data retrieval method, named as HSBEE CBC. Here, the study encrypts data by utilizing ECC technique. Further, the study utilized CBC (Cosine based clustering) method for these clustering those encrypted data. For improvising the security, the study evaluated trust for the users, who tries to retrieve the data. After trust evaluation, the study decrypts the data. Moreover, the study evaluated the performance of recommended method and compared it with other conventional methods.

As cloud computing technologies possess various security challenges, the users couldn't use its full potential. Further, storing sensitive data was considered to be insecure. Even though several methods were developed in the past, none of them have maintained end to end security. Also, the already existing techniques couldn't solve key intricacy. Therefore, to overcome these limitations as well as ensuring DT (Data transmission), [26] suggested a secured data transmission method with the aid of data de-duplication as well as distributed cloud server. The study conducted experimental analysis for analysing the performance of the recommended method. The outcomes of the study revealed that the introduced method performs much better than already existing methods.

Generally, the cloud storage auditing method is utilized for verifying data integrity in cloud. Such that, [27] exploited Diffie Hellman technique for exchanging the key in TPA for improvising the auditing performance. Further, the generated key in third-party auditor is shared as encrypted key within user. The ephemeral key was generated by Diffie Hellman, which seemed to be significantly fast in the generation of new key-pairs. The suggested method has been evaluated in simulated environment, as well as the study compared it with other existing models. The outcomes stated that the presented method has accomplished better performance (1.1s) than prevailing method (1.19s).

A secured multi keyword ranked searching technique over encrypted cloud data that performs dynamic update operations such as insertion as well as deletion of documents has been introduced by [28]. Particularly, the widely utilized TFIDF method as well as vector space model were integrated in query generation and index construction. Further, the clusters were documented by the presented hierarchical method on the basis of minimal relevance threshold. Because of utilization of tree based index architecture, the suggested method could accomplish sub linear search time, and also could deal with document insertion and deletion. Finally, the study performed more experiments for demonstrating the efficacy of the presented method.

[29] suggested a suitable scheme in the CC. The method eradicates a most of the computational work by means of including in public system parameters apart from transferring in encryption. Apart from that a cipher text test phase have been done before decryption that avoids huge computational overhead because of prohibited cipher texts. The work utilized a chameleon hash function for the generation of immediate cipher text. The security and efficiency of the proposed schema have been proved by means of wide performance analysis. A POCC system (privacy preserving outsourced classification in CC) has been recommended by [30] for the preservation of data confidentiality. This evaluator could able to train securely a classification setup on the encrypted data with various public keys that are being outsourced from the several information's. And thereby our scheme has been proved to be more secure in the aspect of semi honest model. The datasets that were possessed by the multiple data owners in the cloud were employed with the deep learning methodology. But before employing the deep learning technique the two most significant challenges prevailing need to solved. The first challenge is that every operation which includes the intermediate results need to be secured in an appropriate manner by encrypting the data with various keys. And minimizing the cost required for computation and communication with the data owners serves the next challenge. The above mentioned challenges were solved by proposing two different methodologies in the research work. First a MK-FHE (i.e.) Multi-Key Fully Homomorphic Encryption was proposed as a basic methodology followed by proposing an advanced methodology which depends upon the hybrid structure that integrates the process of double decryption and FHE (i.e.) the Fully Homomorphic Encryption. And at last, it was evidenced that the two proposed multi-key privacy preserving methodologies for the deep learning provides improved security for the data that were encrypted by [31]. An intelligent approach of cryptography was developed by [32] and due to this proposed approach the cloud service operators could not reach the partial data directly. The file gets divided and stores the data separately in the servers of the distributed cloud computing. Then for determining whether the data packets require the division of files in order to reduce the operation time, an alternative technique with the name of SA-EDS model (i.e.) Security-Aware Efficient Data

Distributed Storage model is devised. This scheme is devised based on various other algorithms proposed in the work like the AD2 (i.e.) Alternative Data Distribution Algorithm, SED2 (i.e.) Secure Efficient Data Distribution Algorithm and EDC on (i.e.) Efficient Data Conflation Algorithm. Both the efficiency and security measures were analyzed based on the experimental evaluations. And from the results of the simulations, it can be concluded that the proposed work possesses the capacity to provide protection to the clouds from various threats in an efficient manner and then the computational time was also reduced to a satisfactory range.

An enhanced novel technique match-then-encrypt was recommended by [33] which established a matching phase in between encryption and decryption. By computing special components in cipher texts this proposed techniques has been worked which are utilized to evaluate the test when the private key of the attribute matched the hidden access policy without decryption. During decryption particular attribute secret key components are generated which enables the aggregation of pairings for the fast decryption. This paper proposed an anonymous ABE construction and then attained a security-enhanced extension on the basis of unforgeable one-time signatures. The matching test computation cost is lower than decryption operation which required only small and constant number of pairings. Finally, comparison and security analysis of the proposed work ensured the attribute privacy and enhanced decryption efficiency in mobile cloud computing for data storage which are outsourced.

2.3. Multi-tenant

In recent years, several studies discussed opportunities and issues of network function virtualization conveys to multi–tenant cloud. A cloud architecture was suggested by [34] that derives the benefits from virtual network functions. More tenants released their application based on cloud regarding cloud's performance, management and security. The cloud provider deployed various hardware middle boxes which are essential to the cloud, anxieties has been increased regarding their cost, performance and manageability. To overcome these issues virtual network function was proposed. Finally, it served as an enlightened for furthermore efforts. An control model for accessing the multi-tenant cloud based services by utilizing the access control model that depends upon the attributes was introduced by [35] and the use-cases are provisioned for the purpose of analyzing the cloud services. Following that, an exchanging tokens method was employed for extending a unique model for the scenarios of Inter cloud. An effective mechanism was applied for converting very complicate logic expressions in order to design a very compact decision diagrams and also for facilitating the evaluation of policies based on the attributes. Based on the multi-tenant technique, a prototype for accessing the control system of the Inter cloud is framed, verified and finally combined onto the project of GEYSERS. Corresponding assessments were carried out and it can be verified that the proposed work possess better performance by means of number of clients and cloud resources.

The performance of the software system in the cloud computing is improved by [36] through an efficient framework and it also performs inspection and evaluation for improving the performance. The simulation tasks with abstract descriptions were converted to particular necessities of the requirements by means of the quality and quantity. This conversion is carried out by establishing a radial based function neural network. Then very complicated process of resource allocation in a multi-tenant cloud computing environment is represented by constructing an innovative mathematical model which considers the satisfaction of tenants based on the priority, multi-level load balance and overall cost taken for computation. Depending upon various K-means methods and elitist archive, an improved multi objective genetic algorithm is proposed with the intention of attaining optimal allocation of resources. The prototype of cloud simulation gets required effective support and the computational requirements of the tenants in a distributed environment are satisfied by the proposed methodology.

When an infrastructure-as-a-service cloud was presented as an affordable substitute to handling in-house information methodology, but doesn't give rise to specialized fully prepared-to-utilize features for implementation governance. Contrarily, PaaS- a Platform as a Service system offers utilization governance and provides a service catalog that could be conveniently used by programmers to administer their implementations on a cloud basis. This methodology too offers DevOps tools to help and manage the lifecycle of an answer. [37] provided few ideas concerning the advantages and obstacles that programmers would encounter when deploying a PaaS, who might desire to deliver services or build apps. On IBM Bluemix, which was a PaaS system, this methodology details the stepwise mannered operation of offering services and creating software. They too recognize the essential elements for reaching safety operation, multi-tenancy, and scalability. They also illustrate the planning operation via 2 Bluemix application case studies: RaaS-Rating as a Service and Business process service preview release. The integrity and confidential of the data present in the migration of workload in multi-tenant cloud architecture was attained by [38] via a novel architecture in the research paper. A secured relationship among the sources of the tenants and destination of the data centers were ensured by the proposed architecture along with the staging area. The workload present in various hypervisors were migrated with the help of the above mentioned staging area. The security guidelines were satisfied by the process of migration from the commencement to the conclusion.

3. Proposed Work

Multi tenancy in cloud refers to the group of cloud users who share a common access to data, resources, configurations and other infrastructures with their specific access privileges. Multi tenancy provides two sided benefits

to the users and to the cloud service providers by sharing cloud services and the resources. Even though adapting multi tenancy in cloud architecture brings added advantages to the cloud computing architecture, there are some of the limitations that are still unresolved in the cloud architectures. One of the main problems faced in cloud computing architectures are the task scheduling issue. The next major issue in the cloud architecture is the security issue which has to be also dealt in the multi-tenant cloud architecture. These issues have to be tackled to create a multi-tenancy architecture.

The above mentioned issue are taken into consideration and a novel multi-tenant cloud framework is proposed. A novel modified ECC encryption/decryption technique is proposed to solve the security issues which will also provide a secure key generation and a key transfer methodology. The flow involved in the proposed MECC algorithm is depicted below in the Fig.1.

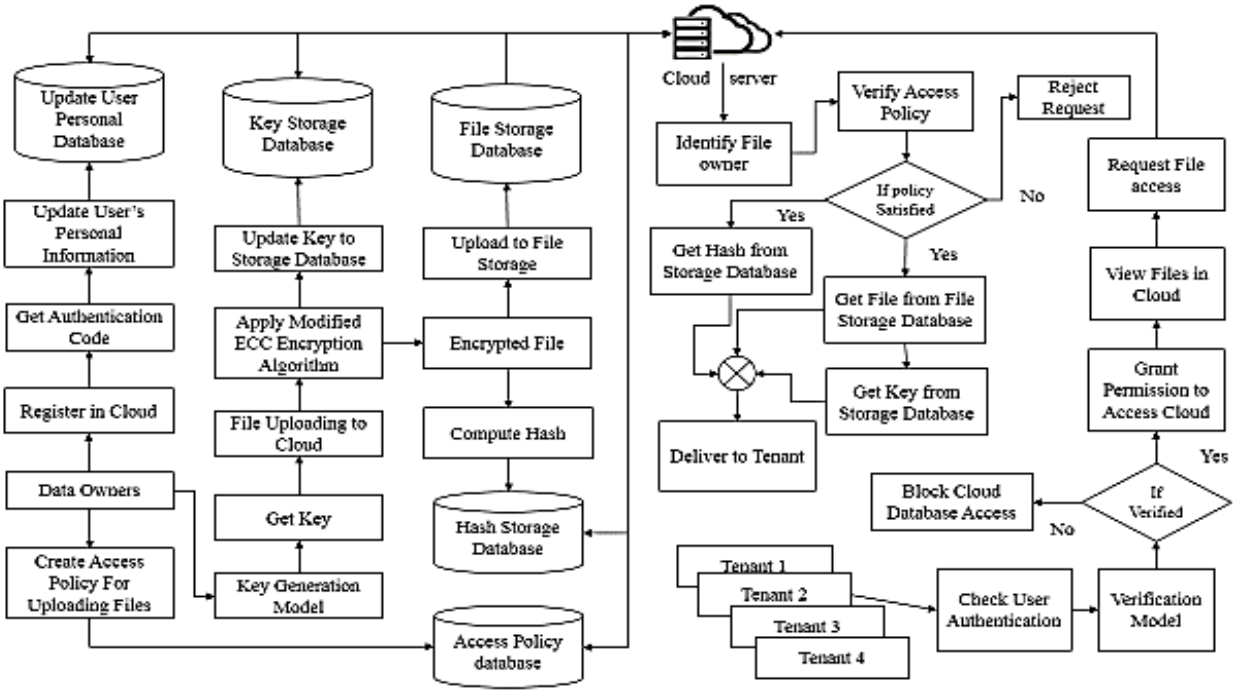

Fig.1. Workflow of the proposed Modified Elliptic Curve Cryptography (MECC)

The data owners are the authorized cloud users who are registered with the cloud and they can use the cloud for secure file storage. The data owner's files are encrypted with the proposed Modified Elliptic Curve Cryptography (MECC) encryption algorithm and the key for encryption is generated by a secure key generation model and the generated keys are stored in the key storage database with the data owner's identity. The encrypted files are stored in the file storage database. To avoid the data loss and to ensure integrity, the hash of encrypted files is stored in the hash storage database. The data owner's personal information's are anonymized and securely stored in the user's personal database. The data owners can be able to customize the file access privileges of the tenants who use the data owner's files or other data by formulating a set of access policies for the data's which he/she uploads in the cloud. An individual or enterprise consisting of huge volume of private data has been referred as data owner. Restricted storage space because of maximized computations prevails within the server configuration of the data owners. Communication module links the cloud databases to provide a single integrated database management system. The submitted user query has been classified into read-write and read only queries [39]. The whole data base is being is controlled by database management system by altering the query thereby promoting effective resource utilization. Generally, users are the entities who utilize several cloud data and applications provided by data owners. The users could able to download a cipher text from the corresponding server.

Data owner upload huge data into the cloud storage and the ECC based DH encrypts with a key. When key request has been sent by the user to the cloud, corresponding key has been sent to the user through mail. After reception of the query the system explore to the data of data owner 1 for precise result. If not found it continues the process with other data owners. After obtaining relevant data the information has been sent to the user with prompt decryption key.

3.1. Proposed Modified Elliptic Curve Cryptography (MECC)- workflow

In the proposed system, reliable encryption has been performed by employing the advantages of ECC and DH algorithm such as increased security and decreased number of key exchange operations. This hybridized algorithm overcome the prevailing limitations such as overhead, larger key size etc., and utilizes DH for key generation.

When a tenant is in need of the data that is uploaded in the cloud database, the request is initially forwarded to the cloud server, where a verification model is proposed that performs checking for ensuring the originality of the

requesting tenant. Once he/she is a verified user, the file visibility is enabled to the user. If the tenant needs to have a direct access to the file, the access policy verification is carried out, and therefore the tenant users who possess the access permissions are only allowed to access the cloud files. A secure key transfer is done to decrypt the file that are uploaded as an encrypted copy to the cloud and along with this a hash key file is given to the tenant user to ensure file integrity. The above proposed novel techniques improve the performance of multi-tenancy in cloud architecture. The proposed techniques are compared with the other state-of-art techniques on the scale of performance, efficiency, encryption time, decryption time, computation time for upload, computation time for download and the cryptography.

MECC algorithm offers high security in cloud data storage and employ symmetric encryption technique for reliable data encryption. In this study an elliptic curve function based Diffee Hellman has been utilized for securing information. The advantages of using MECC algorithm is the employment of small sized key for encryption. The presented MECC framework shown in below pseudo code of table 1, initially it generates the client-server public and private key pairs. After initialization process, the keys are securely shared between the server and the client using MECC. Initially, plain text was encrypted with public key using ECC and converted to cipher text. Then the private key has been categorized into two based on their size. Followed by these the generated two keys will be encrypted by DH and stored in Cloud. So ECC key comprise of two keys that has been encrypted by DH. For decryption, the corresponding two keys would be decrypted by DH and integrated. Finally, the key would be decrypted by ECC thereby plain text will be obtained in a more secured way when compared to conventional methods.

Pseudo Code

Table 1. Pseudo Code for the proposed MECC algorithm

Step 1: Initialization

$D_o \leftarrow data\ owner$

$C_{sp} \leftarrow Cloud\ service\ provider$

$Doac \leftarrow data\ owner\ authentication\ code$

$Doac = generate\ message\ authentication\ code\ for\ data\ owner$

$Sd \leftarrow select\ data$

$Puk \leftarrow public\ key$

$\Pr k \leftarrow private\ key$

$\Pr k = len(prk)/2$

$Puk = prk * p$

Step 2: MECC Encryption

$Ed \leftarrow encrypted\ data$

while Sd data

Ed = Sd.data + (k * Pu) * Fl

End while

Step 3: Access Control Policy

$Nod \leftarrow number\ of\ data$

$for\ i = 0\ Nod\ do$

$Sd = select\ data$

End for

$Tl \leftarrow tenant\ list$

$St \leftarrow selected\ tenants$

$for\ i = 0\ Tl\ do$

$St = selected\ tenants$

End for

Step 4: Create access control policy

$Doac \leftarrow data\ authentication\ code$

$Dac = generate\ message\ authentication\ code\ for\ selected\ data$

$Uac \leftarrow user\ authentication\ code$

$Uac = generate\ message\ authentication\ code\ for\ user$

$Nod \leftarrow number\ of\ data$

$for\ i = 0\ Nod\ do$

$Sd = select\ data$

$End\ \ for$

$Rh \leftarrow Get\ hash\ for\ the\ data\ from\ Csp$

$Get\ key\ for\ the\ data\ from\ Csp$

$Get\ requested\ data\ from\ Csp$

$Doacrd \leftarrow data\ authentication\ code$

$Dac\,rd = generate\ message\ authentication\ code\ for\ received\ data$

$Hr \leftarrow hash\ result$

$if\ Dacrd = Rh\ then$

$Hr = hash\ verified$

$Else$

$Hr = hash\ not\ verified$

$End\ if$

Step 5: MECC Decryption

$CT1 \leftarrow cipher\ text1$

$separate\ decryption\ \ for\ the\ two\ keys$

$CT1 \leftarrow Key1\ \ from\ the\ DH$

$CT1 \leftarrow Key2\ \ from\ the\ DH$

$CT = CT1 + CT2$

$Ed \leftarrow decrypted\ \ data$

$CT1 = k * p$

$while\ Ed\ \ data$

$End\ \ while$

3.2. Mathematical Model of the Proposed System

ECDH is a key exchange method for the determination of the public key and private key. Both the recipient and sender perform the similar operation with entirely different public key and private key, but obtains similar results finally. The following are the mathematical models in accordance with the proposed system.

4. Results and Discussion

Performance analysis are carried out for different performance measures such as encryption time, decryption time, computation time for upload and computation time for download.

4.1. Encryption

Data encryption converts the one form of data to another form of data or in the form to be readable only by the key authorized people. The unencrypted data is known as the plain text and the encrypted data is named as the cipher text.

The Table 3 illustrates the encryption time of the proposed MECC method, from which it is observed that, the proposed method has been compared to RSA, MRSA, MRSAC as well as other existing methods [40] in terms of diverse key length such as 100, 128, 256, 512, 1024, 2048 and 4096. The encryption time of the proposed method was significantly less (5ms) when compared to other existing methods for key length 100bits. Particularly, the encryption time of MRSA method was very high for (222ms) for generating key. When considering the key length 4096 bits, the encryption time of the proposed MECC system was 51ms, whereas the existing method had 92ms as encryption time.

Table 2. Mathematical Model of MECC

1) $E = \{(g, h | h^2 = g3 + ag + b)\{0\}\}, where\ 0 = point\ at\ infinity$

2) $s = \frac{h_B - h_A}{g_B - g_A} \bmod Prime$

3) $g_C = (S^2 - (g_A - g_B)) \bmod Prime$

$g_C = split\ the\ key\ into - len(h_C) / 2000$

4) $h_C = (S - (g_A - g_{R.})) - y_P$

$h_C = split\ the\ key\ into - len(h_C) / 2$

5) $A + A = C = 2A$

6) $S = \frac{3g^2 A + a}{2h_A} \bmod Prime$

7) $g_C = (S^2 - 2g_A) \bmod Prime$

8) $h_C = (S(g_A - g_C) - h_A) \bmod Prime$

9) $A + B = 0\ if\ (g_A = g_B)$

10) $A + B = 0\ if\ (g_A = 0)$

11) $A \in E; k \in Z$

$B \in kA$

12) $B = A + A + \ldots + Ak\ \varepsilon\ Z$

Table 3. Encryption time

Key length (in bit)	Existing	MRSA	MRSAC	Proposed
100	10	222	188	5
128	12	205	305	8
256	15	329	409	10
512	19	1672	2762	15
1024	30	11,625	13,625	24
2048	50	99,891	10,880	39
4096	92	1,10,907	21,887	51

4.2. Decryption

Data decryption is the method of processing the encrypted or encoded text and converting it back in to an original text or data using suitable keys which are generated for the easier understanding by the computer or the person.

Table 4. Decryption time

Key length (in bit)	Existing	RSA	MRSA	MRSAC	Proposed
100	16	88	107	212	11
128	31	188	122	188	25
256	47	62	156	203	36
512	63	218	968	688	51
1024	78	1,453	6,938	7038	63
2048	109	15,203	53,609	83,709	89
4096	187	18,381	10,957	10,957	159

The Table 4 demonstrates the decryption time of proposed MECC system. It is noticed that, the proposed system has been compared to MRSAC, MRSA, RSA and other prevailing methods in accordance to different key lengths (100, 128, 256, 512, 1024, 2048 and 4096). The proposed MECC method has achieved better decryption time than other existing methods [40]. When considering the key length (100 bits), the decryption time of MECC method was 11ms, whereas the encryption time of MRSAC was 212ms. When considering key length (4096 bits), the decryption time for

the proposed model was 159ms, whereas the decryption time was significantly higher in MRSA and MRSAC models (10,957ms).

4.3. Computation Time for Upload

The time taken for uploading a certain data in the cloud is known as the computation time taken for uploading.

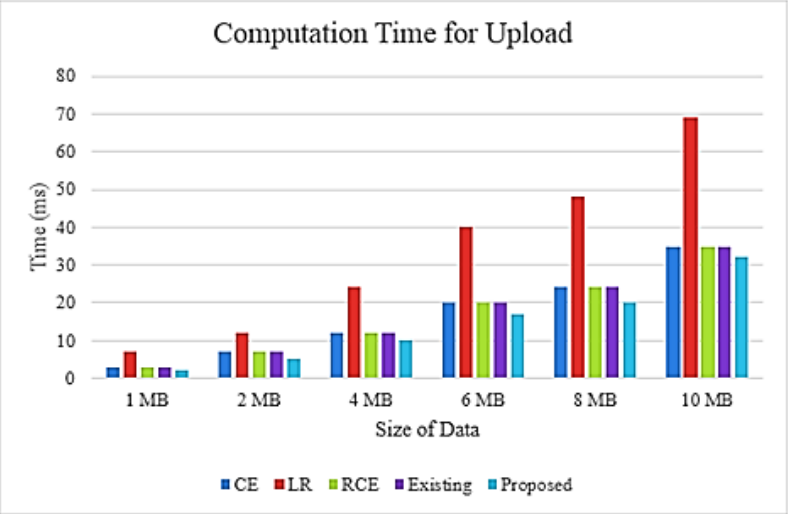

Fig.2. Comparison of computation time taken for upload of proposed MECC with the existing algorithms

Fig. 2 represents the comparison of the computation time taken for uploading a data to the cloud. A comparison is made for the proposed MECC algorithm with the different existing algorithms such as CE, LR, RCE and AES. And from the obtained result it can be inferred that the proposed MECC consumes less computation time for upload

4.4. Computation Time for Download

The time taken for downloading a certain data from the cloud is known as the computation time taken for downloading.

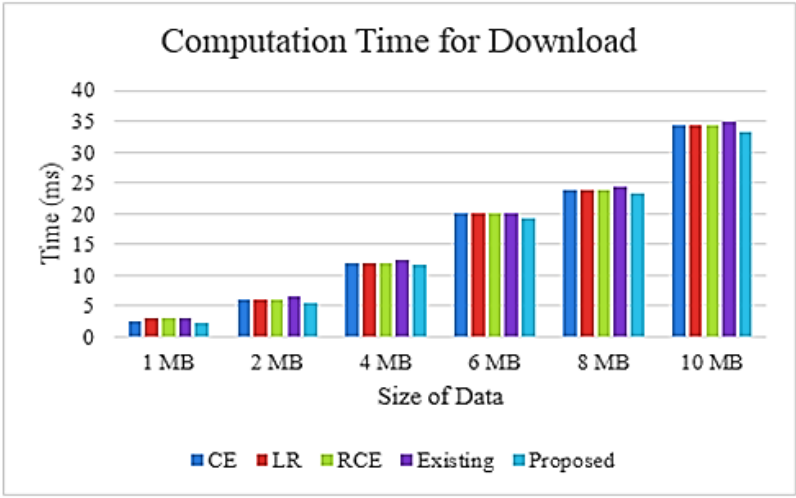

Fig.3. Comparison of computation time taken for download of proposed MECC with the existing algorithms

Fig. 3 denotes the comparison of the computation time taken for downloading a data from the cloud. A comparison is made for the proposed MECC algorithm with the different existing algorithms such as CE, LR, RCE and AES. And from the obtained result it can be concluded that the proposed MECC consumes less computation time for download.

The Fig. 4 deliberates the key generation time, from which it is observed that the proposed MECC method was compared with other prevailing methods such as MRSAC, MRSA, RSA and existing techniques [40] with respect to different key lengths like (100, 128, 256, 512 and 1024). The key generation time for key length (1024 bits) was found to be 35ms. This seemed to be significantly low when compared to 1625ms in MRSAC method. The key generation time was 65ms for key length (100 bits), while the key generation time was higher (153ms) for MRSAC method.

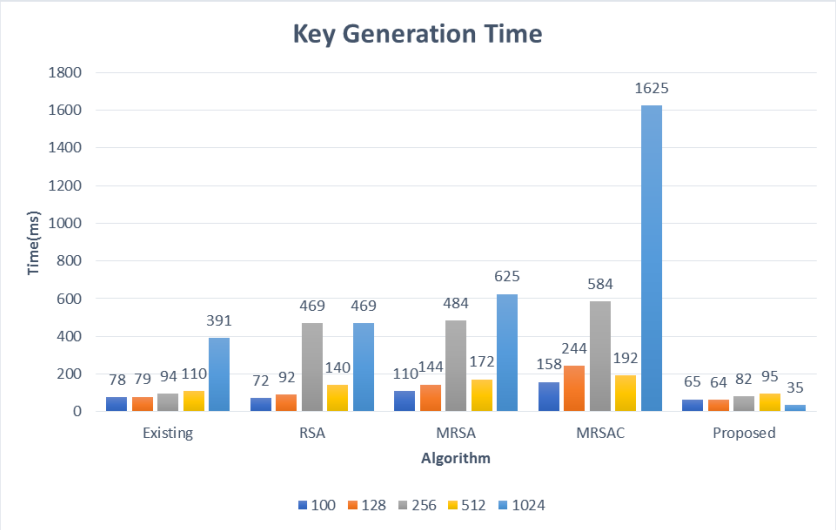

Fig.4. Key generation time

4.5. Cipher Text

A normal text is encrypted for storing it in the cloud and the converted text after the process of encryption is known with the name of cipher text.

Table 5. Comparison of Cryptography for various algorithms

Algorithm	Original Text	Cipher Text	Plain Text
AES	240KB	847KB	240KB
Blow Fish	240KB	955KB	240KB
Two Fish	240KB	955KB	240KB
Proposed	240KB	836KB	240KB

Table 5 illustrates the comparison of cryptography performed for the proposed MECC algorithm with various existing algorithms. And it can be clearly obtained that the cipher text of the proposed MECC algorithm contains less size of the cipher text on comparing with other existing algorithms. The proposed system has reduced cipher text key size of 836KB when compared with the existing AES, Blow Fish, and Two Fish.

5. Conclusions

Enhanced security with reliable time and computational complexity is the urgent need of cloud users. This paper proposed Modified Elliptic Curve Cryptography in a multi-tenant architecture for obtaining outshining cryptography. The alternate keys are generated to grant improvement in the security when comparing the proposed algorithm with the previously existing algorithms. Performance evaluation is carried out for various performance measures like encryption time, decryption time, computation time for upload, computation time for download and cryptography. From the results attained at the end of the simulations, it can infer that the proposed MECC algorithm consumes less time for encryption, decryption, computation for upload and computation for download. Similarly, the cryptography of the proposed MECC algorithm also possess reduced size when comparing with other existing algorithms. Advantages like less memory, high operational performance, small sized keys and rapid key generation process, and effective resource savings enable the proposed system to obtain high efficiency. When considering the key length 4096 bits, the encryption time of the proposed MECC system was 51ms, whereas the existing method had 92ms as encryption time. Similarly, when considering key length (4096 bits), the decryption time for the proposed model was 159ms. Further the key generation time (35 s) also seems to be considerably reduced when compared with the existing methods. Accordingly, the proposed system has reduced cipher text key size of 836KB when compared with the existing AES, Blow Fish, and Two Fish.

References

[1] N. Krishnaraj, M. Elhoseny, E. L. Lydia, K. Shankar, and O. ALDabbas, "An efficient radix trie-based semantic visual indexing model for large-scale image retrieval in cloud environment," *Software: Practice and Experience,* vol. 51, pp. 489-502, 2021.

[2] Zuhi Subedar, Ashwini Araballi. "Hybrid Cryptography: Performance Analysis of Various Cryptographic Combinations for Secure Communication", International Journal of Mathematical Sciences and Computing, Vol.6, No.4, pp.35-41, 2020.

[3] R. Lin, B. Wu, and Y. Su, "An adaptive weighted pearson similarity measurement method for load curve clustering," *Energies*, vol. 11, p. 2466, 2018.
[4] Rosalina, Nur Hadisukmana, "An Approach of Securing Data using Combined Cryptography and Steganography", International Journal of Mathematical Sciences and Computing, Vol.6, No.1, pp.1-9, 2020.
[5] C. M. Mohammed and S. R. Zebaree, "Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS: A review," *International Journal of Science and Business*, vol. 5, pp. 17-30, 2021.
[6] Isma Zulifqar, Sadia Anayat, Imtiaz Khara, "A Review of Data Security Challenges and their Solutions in Cloud Computing", International Journal of Information Engineering and Electronic Business, Vol.13, No.3, pp. 30-38, 2021.
[7] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 1265-1277, 2016.
[8] Muhammad Junaid Arshad, Muhammad Umair, Saima Munawar, Nasir Naveed, Humaira Naeem, "Improving Cloud Data Encryption Using Customized Genetic Algorithm", International Journal of Intelligent Systems and Applications, Vol.12, No.6, pp.46-63, 2020.
[9] Kapan Oralgazyolu Shakerkhan, Ermek Tolegenovich Abilmazhinov, "Development of a Method for Choosing Cloud Computing on the Platform of Paas for Servicing the State Agencies", International Journal of Modern Education and Computer Science, Vol.11, No.9, pp. 14-25, 2019.
[10] R. Masram, V. Shahare, J. Abraham, and R. Moona, "Analysis and comparison of symmetric key cryptographic algorithms based on various file features," *International Journal of Network Security & Its Applications*, vol. 6, p. 43, 2014.
[11] Jayashree Agarkhed, Ashalatha R., "Security and Privacy for Data Storage Service Scheme in Cloud Computing", International Journal of Information Engineering and Electronic Business, Vol.9, No.4, pp.7-12, 2017.
[12] Muhammad Yousaf Saeed, M.N.A. Khan, "Data Protection Techniques for Building Trust in Cloud Computing", International Journal of Modern Education and Computer Science, vol.7, no.8, pp.38-47, 2015.
[13] Mohit Agarwal, Gur Mauj Saran Srivastava, "Cloud Computing: A Paradigm Shift in the Way of Computing", International Journal of Modern Education and Computer Science, Vol.9, No.12, pp. 38-48, 2017.
[14] K. Umamaheswari, S. Sujatha, "INSPECT- An Intelligent and Reliable Forensic Investigation through Virtual Machine Snapshots", International Journal of Modern Education and Computer Science, Vol.10, No.3, pp. 17-28, 2018.
[15] B. P. Rimal and M. Maier, "Workflow scheduling in multi-tenant cloud computing environments," *IEEE Transactions on parallel and distributed systems*, vol. 28, pp. 290-304, 2016.
[16] A. Furda, C. Fidge, A. Barros, and O. Zimmermann, "Reengineering data-centric information systems for the cloud–a method and architectural patterns promoting multitenancy," in *Software Architecture for Big Data and the Cloud*, ed: Elsevier, 2017, pp. 227-251.
[17] A. Patil, "Enhanced-Elliptic Curve Diffie Hellman Algorithm for Secure Data Storage in Multi Cloud Environment," *International Journal of Intelligent Engineering and Systems, DOI*, vol. 10.
[18] V. Chang, Y.-H. Kuo, and M. Ramachandran, "Cloud computing adoption framework: A security framework for business clouds," *Future Generation Computer Systems*, vol. 57, pp. 24-41, 2016.
[19] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: a survey," *Future Generation Computer Systems*, vol. 56, pp. 684-700, 2016.
[20] K. Gai, M. Qiu, H. Zhao, L. Tao, and Z. Zong, "Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing," *Journal of Network and Computer Applications*, vol. 59, pp. 46-54, 2016.
[21] F. Jalali, K. Hinton, R. Ayre, T. Alpcan, and R. S. Tucker, "Fog computing may help to save energy in cloud computing," *IEEE Journal on Selected Areas in Communications*, vol. 34, pp. 1728-1739, 2016.
[22] B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions," *Future Generation Computer Systems*, vol. 79, pp. 849-861, 2018.
[23] F. S. Ali, H. N. Saad, F. H. Sarhan, and B. Naaeem, "Enhance manet usability for encrypted data retrieval from cloud computing," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, pp. 64-74, 2020.
[24] P. Kumar and A. K. Bhatt, "Enhancing multi-tenancy security in the cloud computing using hybrid ECC-based data encryption approach," *IET Communications*, vol. 14, pp. 3212-3222, 2020.
[25] R. Swami and P. Das, "An effective secure data retrieval approach using trust evaluation: HBSEE-CBC," *International Journal of Information and Communication Technology*, vol. 17, pp. 403-421, 2020.
[26] D. V. K. Vengala, D. Kavitha, and A. S. Kumar, "Secure data transmission on a distributed cloud server with the help of HMCA and data encryption using optimized CP-ABE-ECC," *Cluster Computing*, vol. 23, pp. 1683-1696, 2020.
[27] R. K. Yarava and R. P. Singh, "Efficient and Secure Cloud Storage Auditing Based on the Diffie-Hellman Key Exchange," *International Journal of Intelligent Engineering and Systems*, vol. 12, pp. 50-58, 2019.
[28] A. Indhuja, R. B. M. V. Shaik, and P. Sujatha, "A multi-keyword ranked search scheme over encrypted based on hierarchical clustering index," *International Journal on Smart Sensing and Intelligent Systems*, vol. 10, 2017.
[29] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Computers & Security*, vol. 72, pp. 1-12, 2018.
[30] P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen, and K. Chen, "Privacy-preserving outsourced classification in cloud computing," *Cluster Computing*, vol. 21, pp. 277-286, 2018.
[31] P. Li, J. Li, Z. Huang, T. Li, C.-Z. Gao, S.-M. Yiu, *et al.*, "Multi-key privacy-preserving deep learning in cloud computing," *Future Generation Computer Systems*, vol. 74, pp. 76-85, 2017.
[32] Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, "Intelligent cryptography approach for secure distributed big data storage in cloud computing," *Information Sciences*, vol. 387, pp. 103-115, 2017.
[33] Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, and I. You, "Ensuring attribute privacy protection and fast decryption for

outsourced data security in mobile cloud computing," *Information Sciences*, vol. 379, pp. 42-61, 2017.
[34] R. Yu, G. Xue, V. T. Kilari, and X. Zhang, "Network function virtualization in the multi-tenant cloud," *IEEE Network*, vol. 29, pp. 42-47, 2015.
[35] C. Ngo, Y. Demchenko, and C. de Laat, "Multi-tenant attribute-based access control for cloud infrastructure services," *Journal of Information Security and Applications*, vol. 27, pp. 65-84, 2016.
[36] G. Peng, H. Wang, J. Dong, and H. Zhang, "Knowledge-based resource allocation for collaborative simulation development in a multi-tenant cloud computing environment," *IEEE Transactions on Services Computing*, vol. 11, pp. 306-317, 2016.
[37] M. Kim, A. Mohindra, V. Muthusamy, R. Ranchal, V. Salapura, A. Slominski, *et al.*, "Building scalable, secure, multi-tenant cloud services on IBM Bluemix," *IBM Journal of Research and Development*, vol. 60, pp. 8: 1-8: 12, 2016.
[38] S. Manikandasaran and S. Raja, "Security Architecture for multi-Tenant Cloud Migration," *Int. J. Future Comput. Commun*, vol. 7, pp. 42-45, 2018.
[39] K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining data owner-side and cloud-side access control for encrypted cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 13, pp. 2062-2074, 2018.
[40] E. Subramanian and L. Tamilselvan, "Elliptic curve Diffie–Hellman cryptosystem in big data cloud security," *Cluster Computing*, pp. 1-11, 2020.

Authors' Profiles

S. Udhaya Chandrika graduated from Annamalai University. She is currently working in IBM, Chennai.

Dr. T. Pramananda Perumal was a Principal (Retd.), in Presidency College in Chennai. His qualifications are M.Sc., PGDCA., Ph.D. (Computer Science & Engg.).

How to cite this paper: S. Udhaya Chandrika, T. Pramananda Perumal, "Modified ECC for Secure Data Transfer in Multi-Tenant Cloud Computing", International Journal of Computer Network and Information Security(IJCNIS), Vol.14, No.6, pp.76-88, 2022. DOI:10.5815/ijcnis.2022.06.06