Middle-East Journal of Scientific Research 25 (1): 117-127, 2017
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2017.117.127

Effective Secure Data Storage in Cloud by Using ECC Algorithm

[1]S. Sridharan and [2]A. Arokiasamy

[1]Dept. of CSE, University College of Engineering, Thirukkuvalai, India
[2]Dept. of CSE, E.G.S.Pillay Engineering College, Nagappattinam, India

Abstract: Cloud computing is a rising field in the information technology (IT) industry because of its performance, low cost, high availability and much more. Cloud providers offer several storage services for their users in an efficient manner. Cloud users are allowed to store their data on cloud server using cloud storage and reduce the burden of storing and retrieving in the local machine. The data leakage, lack of proper security control policy and weakness in the data entry are the main worries of the companies. So that a cloud data security models should be able to overcome all the possible issues of cloud computing, so as to provide the benefits of cloud computing and preventing the owner's data from all the risks associated. We intend to propose a secure cloud storage system ECC algorithm for encryption and decryption process. Initially, the user sends a request to the cloud server provider (CSP) for storing a file in a cloud. In this phase we will give one password to the user and verification sign also have some security level questions. Then the CSP will verify that data and accept that file and encrypt that file and stored on the cloud server. If the user wants that file means they send a request to CSP also they will send a password and send a verification signature and some security level questions after they will decrypt the file and send to the user.

Key words: Cloud server provider · ECC · Decrypt · Cloud computing · Security · Encryption

INTRODUCTION

Of late, the Cloud computing has been doing its elegant rounds as an appealing candidate in the vital domains of industry and academia. It brings in a novel concept of fascinating business pattern and computing model, which effectively facilitates the on-demand provisioning of computational and storage resources. A further ray of hope in the pathway of improvisation in the safety aspects in the arena of cloud computing radiates in the garb of cryptographic approaches. Plagued by a host of constraints in the computational efficacies and the related challenges, the time-tested cryptographic methods have miserably failed to make an aggressive and impressive thrust in the cloud-dependent scenarios. There is no second opinion regarding the fact that the data constitutes a critical asset for any kind of organization, which may appear in several versions such as the numbers, words, images and all that [1]. With the result, the data confidentiality and safety have surfaced as significant challenges encountered by almost all entities [2,3]. Further, the data is invariably concerned with diverse parameters like the precision, legitimacy, consistency and so forth. The superior-level safety facets on the deployment and the admittance to cloud services and resources have to be rationally alienated from the service itself and have to be represented in such a manner that they are interoperable with the diverse inferior safety systems of the cloud providers. Further, the functional and financial advantages of the cloud are wide-ranging and unfathomable.

Nevertheless, the safety guarantee and lucidity persist as pertinent problems in facilitating the customer confidence in the cloud service providers (CSPs).

Both the captioned challenges emerge as further complicated to effectively deal with the two specified features such as the zooming number of CSPs furnishing the wide-ranging cloud- enabled services, right from virtual machines and storage to transactional databases, as well as the novel architectures controlling the services

Corresponding Author: S. Sridharan, Department of CSE, University College of Engineering, Thirukkuvalai, Tamilnadu, India. E-mail: sridharresearch2016@gmail.com.

of multiple CSPs. The sophisticated cloud computing techniques are taking the world by storm, with the incessant shower of sea changes with the unprecedented and unbelievable impacts on the human society since the inception of the human species, with an influential section of the elite taking the fullest advantages of the captioned services, almost always without their knowledge. For instance, whenever an individual carries out a Google search, registers a remark on a preferred social networking site, or effectively employs a smartphone, he virtually becomes a client of the cloud service provider. In the current golden era of Cloud Computing, galore are the prospects which easily facilitate the data stored distantly to be momentarily cached on the laptops, tablets, smartphones, or the parallel sophisticated internet gadgets. The software industries and the users who park their data in the cloud are significantly adaptable and enjoy certain advantages such as the evasion of huge capital outlay on the individual upkeeps, hardware, software and respite from the online weight of data storage. The Cloud Computing pattern appreciably offers appealing and superlative service to their clients. In fact, the cloud computing represents a web-dependent computing wherein a host of far-flung servers are networked to facilitate the centralized data storage and online accessibility to the computer services or resources. The cloud has incredibly widened its web and, as a result, has emerged as a very dominant gadget which is well-geared to furnish added resources to a wide spectrum of data-hungry clients. Nevertheless, it is very vital to maintain the secrecy of the files in the cloud as a non-reliable third party.

By the term ‘cloud computing’ what is meant is the enlargeable and on demand services which are offered on a platter through the magnificent medium of the web from the highly sophisticated data centers. It has become a cynosure of attention in the realms of the data systems and computer science disciplines. It zealously continues its journey of victory and accomplishment and has almost arrived at the commercialization stage of its rocking growth. A feast of diverse commercial cloud providers vies with one another in presenting a multitude of services, ranging from the IaaS to the SaaS, to attract the clients and offer them the facility of access to augment the cloud services for diverse purposes. The cloud services have established themselves as the indispensable segments of the sophisticated data and transmission mechanisms and exert an immense and forceful impact in the day-to-day life of every Tom, Dick and Harry. The outstanding cloud services ranked top on the list include the mighty Amazon's Simple Storage Service, Box.net, Cloud Safe and the rest.

Literature Survey: With the deft deployment of the cloud storage, the data owners are competent to distantly store their data and avail the on-demand excellent quality cloud services doing away with the need for the local data storage and preservation. Nevertheless, the novel pattern has not generated any safety challenges. One of the vital problems is concerned with the guaranteeing of the honest of the outsourced data. To effectively tackle the related challenge, Jianbing Ni *et al*. [11], launched a significantly effective and vibrant auditing protocol for the cloud storage which claimed a host of several pleasing facets. However, it was proved that the protocol was not safe in the presence of a dynamic opponent in the cloud scenario and the opponent was competent to randomly transform the cloud data hoodwinking the relative auditor in the auditing procedure. However, they were able to offer a fruitful solution to successfully tackle the issue simultaneously safeguarding the entire attributes of the original protocol.

Malina *&* J. Hajny [9] elegantly launched an innovative privacy-preserving safety solution for the cloud services. The novel solution was dependent on an effective non bilinear group signature method furnishing the secret access to cloud services and collective storage servers. Their suggested solution furnished secret verification for the registered users. Accordingly, the personal characteristics of the user such as the age, legitimate registration and effective payment were established without exposing his identity and he was competent to enjoy the cloud services without any causing any threat of profiling their conduct. Nevertheless, if a user violates the rules and regulations of the service provider rules, his right of entry is summarily withdrawn. Their novel solution furnished secret access, non-linkability and the privacy of the communicated data. They effectively performed the solution as evidence of the idea application and offered convincing test outcomes. Moreover, they deeply investigated the modern privacy preserving solutions for the cloud services and group signature schemes as the fundamental modules of the privacy enhancing solutions in the cloud services. An effective analysis and contrast were also made between the feet of their novel with the parallel solutions and methods. A data center represents an infrastructure which effectively

promotes the Internet service. The cloud computing, on its part, on a dynamic spree, sporadically generating sea changes in the domain of the Internet service infrastructure, thereby facilitating several entities to vibrantly configure further sophisticated Web and mobile applications for the multitude of clients by fully exploiting the extent and adaptability of the collective physical infrastructures furnished by cloud computing.

Zhen Chen & Wenyu Dong [3] charismatically launched the system accomplishment of the vCNSMS, which represented a collaborative network security prototype system for the purpose of deployment in a multi-tenant data center. They effectively exhibited the vCNSMS with a central collaborative mechanism and profound packet scrutiny with an open source UTM technique. A safety level dependent safety strategy was envisioned for the purpose of streamlining the safety rule administration of the vCNSMS. In this regard, diverse safety levels were endowed with various packet scrutiny techniques which were imposed with several safety plugins. A well-groomed packet verdict technique was also included in the vCNSMS for the purpose of the intelligence flow processing to act as a shield against the potential network assaults within a particular data center network.

The Internet safety issues habitually crop up as a vital threat with manifold safety constraints like the Internet worms, spam and phishing assaults. The Botnets, which represent well-orchestrated disseminated network assaults, involves a huge number of bots which produce a gigantic quantum of spam or trigger the Distributed Denial of Service (DDoS) assaults on the hapless victim hosts. Further, the sophisticated potential botnet assaults go a long way in deteriorating the level of the Internet safety in an incredible manner.

Zhen Chen Fuye Han & Junwei *l.* [4] excellently launched a realistic collaborative network security management technique by means of efficient collaborative Unified Threat Management (UTM) and traffic probers. They invariably employed the cloud storage to maintain the gathered traffic data for the purpose of subsequent processing by means of the cloud computing platforms to effectively locate the malevolent assaults. As a realistic instance, the phishing attack forensic investigation was offered and the requisite computing and storage resources were assessed depending on the actual trace data. The cloud-based safety center was competent to instruct each collaborative UTM and prober to gather events and raw traffic, forward them back for deep investigation and create novel safety regulations, which were imposed by collaborative UTM and the feedback events of the corresponding regulations were retransmitted to the safety center.

Hongjun Dai & Shulin Zhao [5] deeply discussed the modern chip multiprocessors which were susceptible to the transitory errors triggered by the on-purpose assaults or system inconsistencies, which were further relevant for the titanic and multi-level caches in the cloud servers. In their document, they intelligently introduced a modified/shared replication cache for the purpose of maintaining a redundancy for the most modern accessed and modified shared L2 cache lines. On the basis of the tests performed in accordance with the Multi2Sim, the relative cache with the appropriate dimension was competent to furnish significant data consistency. Further, the cache was instrumental in considerably cutting back the average latency of memory hierarchy for error rectification, with just approximately 20.2% of L2 cache energy expenses and 2% of L2 cache silicon operating costs.

The Cloud Computing is elegantly flagged off as the upcoming generation design of the IT Enterprise. It effectively shifts the application software and databases to the central titanic data centers, where the organization of the data and services is far from satisfactory on account of their non-reliability. The novel approach triggers several novel safety issues, which have not yet been fully comprehended.After careful investigation of the issue of safeguarding the honesty of data storage in the Cloud Computing, Qian Wang &Cong Wang [16], valiantly envisioned the novel concept of entrusting a third party auditor (TPA), in support of the cloud client, to authenticate the honesty of the vibrant data parked in the cloud. At the outset, they located the hassles and the prospective safety challenges of the direct extensions with entirely energetic data updates from the earlier investigations. Subsequently, they brilliantly brought in a novel verification method for the flawless combination of the two vital attributes in their novel protocol blueprint. Especially, for the purpose of highly effective data dynamics, they strived hard to fine-tune the modern evidence of the storage models by effectively managing the classic Merkle Hash Tree configuration for the block tag verification.

The Cloud computing continues to hold sway with ever-zooming significance for the provision of services and accumulation of data on the Internet. Nevertheless,

it is plagued by various important issues which are encountered while shielding the cloud infrastructures from diverse categories of malevolent assaults. What are highlighted here are the safety services offered by a cloud provider as a segment of its infrastructure to its clients (tenants) to effectively ward-off the relative assaults.

Vijay Varadharajan & Udaya Tupakula [15 winningly launched a novel safety design which offered an adaptable safety as a service pattern offered by a cloud provider to its tenants and clients of its tenants. Their safety as a service technique invariably guaranteed a baseline safety to the provider to shield its own cloud infrastructure, in addition to furnishing elasticity to tenants to enjoy added safety functionalities tailor-made to be in harmony with their safety requisites. In their document, they deeply discussed the deft design of the safety architecture with an extensive account of the manner in which various categories of assaults were successfully overwhelmed by the novel architecture. They effectively carried out the safety architecture and offered an effective assessment and the performance appraisal outcomes.

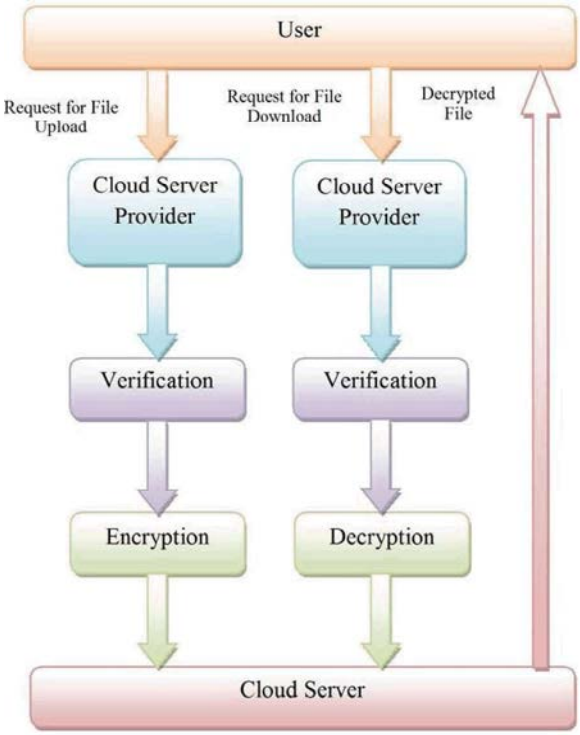

Fig. 1: Proposed Diagram for Cloud Data Security

Problem Identification: The relevance of the cloud computing is in an uptrend, triggered by the ever-zooming nature of the effective utilization of the web-based services. It is well-geared with the requisite skills of offering straight access to the documents, pictures and the media on the cloud storage by means of the cyberspace. With the rapidly increasing success stories in the sophisticated technology market, several specialists are really worried regarding the resultant enhancement in the safety requirements for the cloud computing. Several corporations have initiated strategies on a war- footing to locate and alleviate the current cloud computing safety constraints. Recounted below, in a nutshell, are the general challenges encountered by the modern cloud safety techniques.

- The utmost fundamental deficiency of the cloud computing is network addiction to the internet due to the excessive requirement of the top-speed internet. If the internet connection is sluggish, the download of titanic documents is slated to end in a fiasco.
- The cloud is likely to crop in the course of the transaction and hence the whole activity tends to be a failure if it is delayed and hence it is time-sensitive.
- In the cloud computing, several roadblocks are faced while generating a hybrid technique, if the providers go slowly on providing the service, spelling disaster to the vast majority of cloud users, immensely impacted by the relative deficiency.

The above-cited demerits of several modern techniques have offered the required motivation for commencing the current investigation on the various facets of the Cloud safety.

Proposed Methodology: The cloud storage constitutes a unique pattern of data storage where the digital data is saved in logical pools, the physical storage covers manifold servers and at times locations with the physical scenario being classically owned and administered by a hosting company. The related cloud storage providers are entrusted with the task of preserving the data for the sake of availability and accessibility by the genuine client and maintaining the physical scenario safe and effectively functional. Various entities make outright purchases or take on lease the storage facility from the providers for the purpose of storing client data. The clouds continue to maintain the data secrecy, accessibility, honesty and confidentiality parameters though at times they are

harassed by unscrupulous assaults. Though the effective preservation of suitable data safety is dangling like a Damocles Sword over the heads of the service provider, still a cloud computing infrastructure is well-endowed with the capability of effectively accentuating the general safety. In the document, it is envisaged to launch an innovative and secure cloud storage system viz. the ECC technique devoted for the encryption and decryption function. At the outset, the client prefers an application to the cloud server provider (CSP) for the purpose of storing a file in a cloud. Here, the client is allotted a password and verification sign in addition to asking him certain questions related to the safety aspect. Subsequently, the CSP examines the relative data and accept the file for encryption and subsequent storage in the cloud server. When the client wishes to access the file, he has to forward an application to the CSP who sends a password and a verification signature together with a set of safety-based queries. Subsequently, CSP effectively decrypts the file and forwards it to the client. The innovative technique is performed in the Cloud simulator in the working platform of Java with Windows 7 operating system. Further, we are sure the innovative technique is well-geared to usher in superior and secure data storage by steering clear of the entire safety roadblocks in the process.

Fundamental Characteristics of Cloud Computing:

Self-service on Requirement

The client invariably takes a suitable decision regarding the deployment of computing amenities like the server time and network storage only, in accordance with his ongoing requirements, with no need for superfluous interaction with different service providers.

Broad Network Access

The computing amenities are potentially accessed over the network by effectively utilizing the homogeneous technique which holds up diverse clients, like mobile phones, tablets, laptops and workstations.

Combining of Computing Resources

In addition to the classical virtualization, the cloud computing habitually utilizes the skills of the mechanization of services and multi-tenancy of users at general data resources. The widespread deployment of the identical technological resources is the vital trait of the cloud computing. Prior to the slideshow, the cloud provider is expected to set up separate infrastructures for various users. Nevertheless, with the upsurge of multi- tenancy techniques, it is feasible to offer harmonized pattern, homogeneous regulation in the services, modernization and easier disaster recovery tasks in addition to the effective restoration of the relevant data. Another vital factor is that the data cease to become inevitably associated with a specifically defined strategic location forever, just because they may be concurrently positioned at diverse data centers throughout the length and breadth of the cosmos.

High Elasticity

The client is capable of effortlessly enhancing or reducing the computing capabilities provided by making use of the existing needs. In this regard, the client enjoys unfathomable and unrestricted capabilities.

Data Storage Security in Cloud Computing: The safety of data storage represents the data security on the storage media, which has to be endowed with the qualities of being invariably non-volatile or easily reclaimable after any loss of data whatsoever. In fact, the safety facet has to be afforded due weightage by the software engineers concerned at the time of drawing the blueprint of the cloud storage. It has to encompass both redundant and dynamic data, together with the separation. In this regard, the redundancy has emerged as one of the most vital metrics to safeguard the protection of data storage. And further, the term ‘dynamic’ hints at the fact that the client data is susceptible to variation and hence efficient measures are required to guarantee the reliability of data. Further, the word ‘Separation’ indicates the time of storing the client data in the platform. With an eye on ensuring the autonomous nature of the data, the client is capable of accessing only his own data and any variation in data affected by others have a negligible impact on the existing client. The following section effectively explores the cloud storage topics together with the requirements and safety solutions encircling it.

Cloud Storage: The cloud storage, in turn, constitutes an online disseminated virtual storage offered by the vendor

of cloud computing. The client is competent to access the service of cloud storage by means of the web services interface, or a web-based user interface. In the cloud data storage system, it is not essential to store data locally and the clients are offered the facility of storing their data in the cloud. Hence, the precision and accessibility of the data files have to be ensured before they are stored on the disseminated cloud servers. One of the vital advantages of the cloud storage is its adaptable attribute which enables the client to rent the storage space at any time they need to store their data and they are charged a levy only for the quantity of their utilization. Many entities are able to affect a drastic cut in their expenses and the allied intricacies by storing them in the storage devices with the help of the cloud storage. Just like the cloud computing, the cloud storage boasts of a host of qualities such as the scalability and agility in the cloud storage advantages. However, it also suffers from safety issues, akin to those in the disseminated storage system.

Public Cloud: The substructure of public cloud is intended for use by the public and thrown open to all and here the resources, applications and web services are offered by means of the internet and the public organizations have their valuable contribution in furnishing and supplying the substructures. In practice, a cloud service provider organization exclusively owns the public cloud.

Private Cloud: The private cloud is intended exclusive for use by an organization, with the facility for every personnel in the organization to access data, services and applications while others are denied the facility.

Community Cloud: The community cloud is effectively specified and arranged to offer certain common facilities and resources easily. Its substructure can be swapped among one or multiple institutions. However, the vital issue here is that the works required by them are one and the same though those who require the services pursue more or less identical mission, policy, security and so forth. In the community cloud, a specified group promotes functions such as the safety requisites. Definitely, such type of sharing will have a telling effect on the organization at work

Hybrid Cloud: The most modern pattern is the hybrid cloud, which is the integration of two or more clouds such as the public, private and community clouds. In essence, it is a scenario which employs certain internal and external cloud providers.In the cloud data storage, a client stores his data by means of the CSP into a set of cloud servers, which are functioning in a concurrent, co-operative and disseminated way. The data redundancy can be effectively utilized with the method of erasure-rectification code to additionally take care of the flaws or the server breakdown with the immense growth in the user data both in dimension and significance. Subsequently, for the purpose of the application, the user interrelates with the cloud servers by means of the CSP to access or regain his data. In certain cases, the user has to carry out the block level functions on his data. As the user is not in possession of his data locally, it is of vital significance to offer reassurance to him to the effect that his data is accurately stored and preserved. In certain cases, the user may not possess sufficient time, viability or resources to keep an eye on his data. In the innovative technique, it is presumed that the point-to-point communication channels between each cloud server and the user is authentic and consistent, which may be accomplished in reality with minimum expenses.

User: The users, who possess the data for storage in the cloud and depend on the cloud for data evaluation, encompass both individual consumers and institutions.

Cloud Service Provider (CSP): The CSP in possession of considerable resources and skills in building and controlling the disseminated cloud storage servers owns and manages the live Cloud Computing mechanisms.

Existing Algorithms for Encryption and Decryption for Data Storage Security: The encryption technique has emerged as the most extensively employed approach devoted for the shielding of data within the cloud scenario. The data associated to a client may be classified into two types such as the public and private data. The public data can be shared among the trustworthy clients who offer an open scenario for cooperation. On the contrary, the private data represents the secret data of the client which has to be transferred in the encrypted form for safety and secrecy. Depending on the key attributes, the latest cryptosystem may categorize into two distinct types such as the symmetric and asymmetric cryptosystem. In the case of a symmetric cryptosystem, the sender and receiver share an encryption key and decryption key, which are identical or easy to infer each other. The symmetric cryptosystem encompasses the ECC (Elliptic Curve Cryptography), 3DES, RC5, RC6, Blowfish, Two-Fish and AES (Advanced Encryption Standard. As

far as the asymmetric cryptosystem is concerned, only the receiver is in possession of the public key and private key. While it is possible to expose the public, the private key has to be kept confidential. The asymmetric cryptosystem includes the RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptosystem).

Data Uploading: The uploading of data in the cloud is effectively performed in two distinct sets. The data which is very susceptible is authorized to encrypt before entering the cloud scenarios which is known as the Private data. The private data is encrypted by means of the ECC technique in which the key produced is shared for the purpose of downloading the data. The ECC technique smartly brings in superior-level safety, in a very effective and cost-conscious way. The public data is uploaded as such in the identical version without any variation.

Data Download: The owner of the data is the only person who is expected to download the data uploaded in the private mode. Each and every access to the data is effectively reported by the TPA. The access record encompasses the data being shared or depends on the cloud scenarios. The private data download consists of easy steps as on data upload. The encrypted data is decrypted by means of the key produced while uploading the content. In accordance with the ECC encryption logic, the pair of the key has created the key left for decrypt is for the download. The corresponding decrypt on the data authenticates the veracity of the original data, which goes a long way in authenticating the data safety.

Ecc Based Encryption: An Elliptic Curve Cryptography (ECC) is exploited for the file encryption by creating a personal and public key of encryption in our suggested file. The personal and public keys are produced by the ECC method makes the updated input file more safe as well the produced keys are vigorous. The key generation and formation are explained beneath.

Key Generation by ECC: Elliptic Curve Cryptography (ECC) is as well-known as public key cryptography, which normally has a pair of keys, a public key and a private key and a set of actions associated with the keys to complete the cryptographic operations. The most important advantage of ECC is the small key size. The operations of elliptic curve cryptography are explained over two predetermined fields: Prime field and Binary field. For cryptographic operations, the suitable field is selected with finitely massive number of points. The prime field operations choose a prime number and finitely large numbers of basic points are produced on the elliptic curve, such that the generated points are between 0 to Z. Consequently, we randomly pick one basic point $P_r(R_1,R_2)$ for cryptographic operations and this point pleases the equation of the elliptic curve on a prime field, which is explained as,

$$v^2 \bmod P_{rm} = u^3 + \propto u + \beta \bmod P_{rm} \quad (1)$$

α *and* β are the parameters that labeling the curve and *u and v* are the coordinate values of the generated points *bp* given in Eqn. (1). In order to randomly pick one basic point p_r to carry out the cryptography, it is necessary to select a private key pv_{ky}, which arbitrarily select integers less than pv_{ky} and produce a public key $pu_{ky} = pv_{ky} * p_r$. At this time, every updated file have detached private key pv_{ky} and public key pu_{ky}. The private and public values are inserted and that decimal value is changed into the binary value. Next least important bit is selected, which DataStream is employed for the encryption of the updated motion parameters. Here we are including a firefly algorithm for finding a optimized primary key.

Solutions Representation: In the optimal attribute choice in the decision tree generation, one of the most vital challenges is Concerned with the manner in which the solution has to be represented. The solution illustration ties up with the firefly algorithm accomplishment. We define one firefly (solution) as a possible solution in the population. The initial population of fireflies is generated arbitrarily for the firefly algorithm. The initial population of size Y is defined as follows:

$$A = A_d \, (d = 1, 2, 3 \ldots \ldots n) \quad (2)$$

where, n is the number of fireflies.

The initialized continuous position values are created by means of the following Equation 3.

$$u_k^* = u_{\min} + (u_{\max} - u_{\min}) * r \quad (3)$$

where $x_{min} = 0$, $x_{max} = 1$ and r represents a uniform arbitrary number between 0 and 1.

Fitness Evaluation: The Fitness function is defined in accordance with the motive of the current investigation. Here, an optimization formula is obtained in equation (2), based on the minimization of the objective function as follows

$$w(y) = \min \sum_{i=1}^{m} w(y_i) H_x(y_i) \quad (4)$$

where
$H_x(y_i)$ -> the entrophy
$W(y_i)$ -> the weight of the entropy of each attribute

Firefly Updation: The movement of the firefly (FF) p, when attracted to another more attractive (brighter) firefly q, is evaluated by means of Equation 2 given below.

$$u_p = u_p + ?(r) * (u_p - u_q) + \varnothing(\text{rand} - 1/2) \quad (5)$$

The second term in equation (2) is on account of attraction, the third term introduces randomization with '$\varnothing$' being the randomization parameter and "rand" is a random number produced evenly disseminated between 0 and 1

$$\text{Attractiveness, } Y(r) = e^{-\theta r m}, \; m \geq 1 \quad (6)$$

Where, r represents the distance between two fireflies, γ^0 denotes the initial attractiveness of firefly and θ reveals the absorption coefficient

$$\text{Distance, } r_{pq} = \| u_p - u_q \| = \sqrt{\sum_{k=1}^{d} (u_{p,s} - u_{q,s})^2} \quad (7)$$

where, $u_{p,s}$, represents the s^{th} component of the spatial coordinate of the p^{th} firefly and d denotes the total number of dimensions. Also.,$q \in \{1,2, \ldots F_n\}$ characterizes the arbitrarily selected index. Although q is evaluated arbitrarily, it must be different from p. Here F_n corresponds to the number of fireflies.

Encryption and Decryption: The common form of the safe to store file parameters after the process of encryption is,

$$\gamma = (E_m, C_j) \quad (8)$$

In Eqn. (8), E_m points out the encrypted input files and which is calculated by means of eqn. (9) and C_j as well calculated by means of eqn. (10)

$$E_m = O_m * p_r \quad (9)$$

$$C_j = (u, v) + O_m * (S(P_v)) * P_r \quad (10)$$

In Eqn. (9), O_m symbolizes the original optimized motion parameter and in Eqn. (11), $S(pv_{ky})$ is the private key. These encrypted files are the most important components.

RESULTS AND DISCUSSION

The innovative cloud data security with the aid of ECC algorithm is performed on the working platform of JAVA with Cloud Sim. The size and memory values are also estimated and its average value is contrasted with that of the current method. The table appearing below illustrates the File size value of our proposed study. Table 1 reveals the size taken for each file in bytes. To finish the each File the innovative technique taken size is given in the table. The corresponding value for finishing the 5th file is 5503 original file size if the uploaded size is 795142 then the decrypted size is again 5503. The novel approach finishes the 4th file is 3361 original file size if the uploaded size is 3361 then the decrypted size is 3361. The novel approach finishes the 3th file is 2317 original file size if the uploaded size is 241286 then the decrypted size is 2318. The novel approach finishes the 2th file is 1424 original file size if the uploaded size is 148102 then the decrypted size is 1424. The novel approach finishes the 1th file is 237 original file size if the uploaded size is 24965 then the decrypted size is 237. The graphical illustration is exhibited in Figure 2.

Table 2 reveals the time in ms taken for each file. To finish the each File the innovative technique taken Time is given in the table. The corresponding value for finishing the 5th file is 235791 original file size if the time taken for encryption process is 127605 then the time taken for decrypted process is 117125. The novel approach finishes the 4th file is 97998 original file size if the time taken for encryption process is 18174 then the time taken for decrypted process is 16901. The novel approach finishes the 3th file is 3361 original file size if the time taken for encryption process is 2387 then the time taken for decrypted process is 1404. The novel approach finishes the 2th file is 2317 original file size if the time taken for decryption process is 1483 then the time taken for the decrypted process is 1856. The novel approach finishes the 1th file is 237 original file size if the time taken for decryption process is 2012 then the time taken for decrypted process is 1607. The graphical illustration is exhibited in Figure 3.

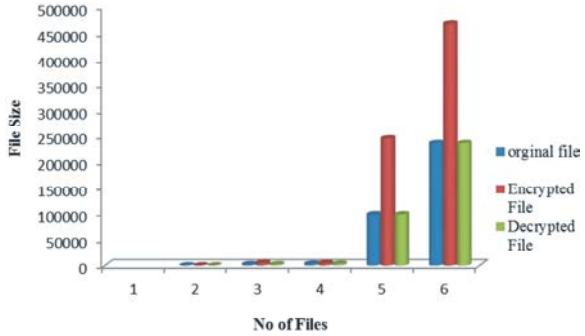

Fig. 2: File Size took for our proposed Method

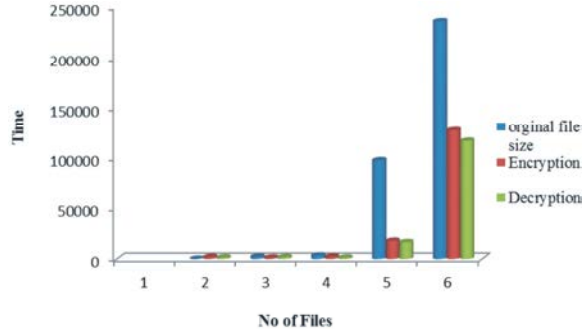

Fig. 3: Time Taken for proposed Method

Table 1: No of Size taken for the Upload and Decryption for our proposed method

Original File Size	File Size After Encryption	File Size After Decryption
237	239	237
2317	5230	2319
3361	4759	3361
97998	244999	97998
235791	467526	235791

Table 2: No of time taken for the encryption and decryption process for our proposed method

Original File Size in bytes	Encryption Time in ms	Decryption Time in ms
237	2012	1607
2317	1483	1856
3361	2387	1404
97998	18174	16901
235791	127605	117125

Figure 3 illustrates the graphical representation of encryption and decryption Time. It is shown in below.

Table 3 reveals the throughput value for each file. To finish the each File the innovative technique taken throughput value is given in the table. The corresponding value for finishing the 5th file is 235791 original file size if the throughput value for upload a file is 1.8478. The novel approach finishes the 4th file is 97998 original file size if the throughput value for upload a file is 5.3922. The novel

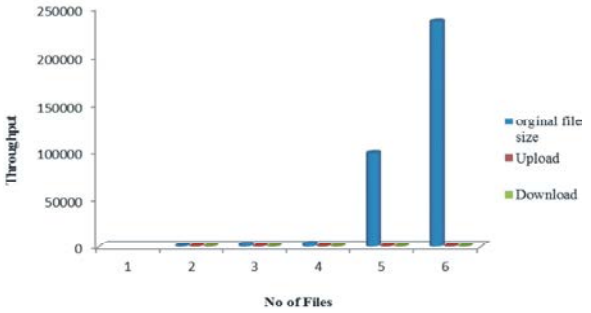

Fig. 4: Throughput value for proposed method

Table 3: Throughput value for Upload and Download for our proposed method

Original File Size	Throughput
237	0.1177
2317	1.5623
3361	1.408
97998	5.3922
235791	1.8478

Table 3: Throughput value for Upload and Download for our proposed method

File Size in (Bytes)	Existing Method Encryption Time in (ms)	Proposed Method Encryption Time in (ms)
160-237	2747	2012
1424-3361	45583	2387

approach finishes the 3th file is 3361 original file size if the Throughput value for upload a file is 1.408. The novel approach finishes the 2th file is 2317orginal file size if the throughput value for upload a file is 1.5623. The novel approach finishes the 1th file is 237 original file size if the throughput value for upload a file is 0.086. The graphical illustration is exhibited in Figure 4.

Comparative Analysis: Here the existing works are compared with our proposed work, in order to prove the proposed work is a better one. For this existing AES is taken to compare the result with our method ECC. The following table is shown the comparative result. The graphical representation of comparative analysis is shown in Figure 5.

Here Figure 5 illustrates the graphical representation of comparative analysis. It is shown in below,

From our results of the comparison, we can say that our proposed work rescues the encryption time. The existing work RSA is taken 2747 ms to complete the encryption in the file size ranges from 160-237, our proposed ECC takes minimum encryption time. It takes nearly 2012 ms to complete the encryption process also in the file size of 160-237. In the second file if the existing

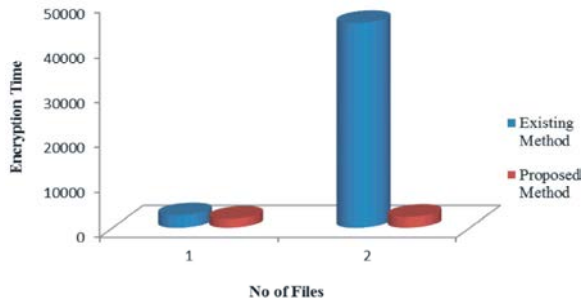

Fig. 5: The graphical representation of comparative analysis

method gives 45583 ms to complete the encryption process in the file size ranges from 628-1424 but in our proposed method gives 2387 ms. From these existing works, we can say that our proposed reduces the encryption time when compared to the existing method.

CONCLUSION

In this secure data cloud, data storage is proposed at the outset with the aid if ECC algorithm for encryption and decryption process. In cloud servers, processors are more vulnerable to soft errors caused by either on purpose attack or system mistakes with the continuous operations. The encryption time of the authors has systematically studied the security and privacy issues in cloud computing based on ECC algorithm. Our proposed secure cloud storage system ECC algorithm for encryption will give a good result when we compare to an existing encryption method using AES. We have identified the most illustrative security/privacy attributes (e.g., integrity, confidentiality, privacy-preservability, availability and accountability), as well as discussing the vulnerabilities, which may be exploited by adversaries in order to perform various attacks. We believe this review will help shape the future research directions in the areas of cloud security and privacy.

REFERENCES

1. Ibrahim Arpaci and Kerem Kilicer, 2015. Effects of security and privacy concerns on educational use of cloud services, ELSEVIER Journal of Computer in Human Behavior, 45: 93-98.
2. Bhubaneswar. 2015. A Review on Cloud Data Security and Its Mitigation Techniques, ELSEVIER Journal of Procedia Computer Science, 48: 347-352.
3. Zhen Chen and Wenyu Dong, 2013. Collaborative Network Security in Multi-Tenant Data Center for Cloud Computing, IEEE Journal of TUP, 19: 82-94.
4. Zhen Chen, Fuye Han and Junwei, 2013. Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System, 18: 40-50.
5. Hongjun Dai and Shulin Zhao, 2015. Security enhancement of cloud servers with a redundancy-based fault-tolerant cache structure, ELSEVIER Journal of Future Generation of Computer System, 52: 147-155.
6. Greg Goth, 2011. Public Sector Clouds Beginning to Blossom Efficiency, New Culture Trumping Security Fears, IEEE Journal of Internet Computing's, 15: 1-9.
7. L.Azua Himmel and F. Grossman, 2014. Security on distributed systems: Cloud security versus traditional IT, IEEE Journal of Research and Development, 58: 3.
8. Jesus Luna and Neeraj Suri, 2015. Leveraging the Potential of Cloud Security Service-Level Agreements through Standards, IEEE Journal of Cloud computing.
9. Malina, L. and J. Hajny, 2015. Privacy-preserving security solution for cloud services", Journal of Applied research and Technology, 13: 20-31.
10. Giuseppe Di Modica and Orazio Tomarchio, 2015. Matchmaking semantic security policies in heterogeneous clouds, ELSEVIER Journal of Future Generation Computer Systems, pp: 1-10.
11. Jianbing Ni and Y. Yong, 2014. On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage, In Proceeding of IEEE Transaction on Parallel and Distribution System, 25: 2760-2761.
12. Passent M. El-Kafrawya and Azza A. Abdo, 2015. Security Issues Over Some Cloud Models, ELSEVIER Journal of Communication, Management and Information Technology (ICCMIT), 65: 853-858.
13. Rizwana Shaikha and Dr. M. Sasikumar, 2015. Data Classification for achieving Security in cloud computing, ELSEVIER Journal of Procedia Computer Science, 45: 493-498.
14. Zahir Tari and Xun Yi, 2015. Security and Privacy in Cloud Computing: Vision, Trends and Challenges, IEEE Journal of Cloud Computing, 2: 30-38.
15. Vijay Varadharajan and Udaya Tupakula, 2014. Security as a Service Model for Cloud Environment, In Proceedings of IEEE Transaction on Network and Service Management, 11(1): 60-75, 2014.

16. Qian Wang and Cong Wang, 2011. Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, In Proceedings of IEEE Transaction on Parallel and Distributed System, 22: 847-859.
17. Wei Wanga and Peng Xu, 2015. A design for cloud-assisted Fair-Play Management System of online contests with provable security, ELSEVIER JOURNAL OF Future Generation Computer Systems, 52: 137-146.
18. Wei Xiao and Peng Xu, 2015. A design for cloud-assisted Fair-Play Management System of online contests with provable security, Journal of Future Generation Computer Systems, 52: 137-146.
19. Zhifeng Xiao and Yang Xiao, 2013. Security and Privacy in Cloud Computing, In Proceedings of IEEE Transaction on Communications System, 15: 843-859.