Turkish Journal of Computer and Mathematics Education *Vol.12 No.2 (2021), 437- 449*

Research Article

Cloud Data Security in Multi Model Attributes For Randomized Key Service Using Encryption Techniques

S.Noordeen[a], and Dr.G.M.Nasira ,

A
Research Scholar,Bharathiar University, Coimbatore- 641 046
bAssistant Professor and Head Department of Computer Applications.,Chikkanna Government Arts College.,Tirupur – 641602.

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: The growing size of information, security became the risk of access from centralized resource providers deploy them into cloud, where authorized users could access them. The nearly combined nature of cloud environment does not yet allow users to perceive the cloud resources and services in a split second. At the same time, they are upgrading. Also, attribute based encryption techniques are used towards the security development in few methods. Also, profile based approaches are used which uses different encryption keys according to user profile. However, all the methods suffer to achieve higher performance in datasecurity. To solve this issue and to improve the security performance, an efficient Service LevelAttributeBasedEncryption (SLABE)ispresented.Inthisapproach,themethoduses different key set of different services. For each attribute, the method maintains different keys for various services. According to the key belongs to the attributes and service, the method performs encryption and decryption. The method improves the performance in security and increases the throughput aswell. Further to improve the security performance, a multi attribute randomized key Service Level Encryption (MARK-SLE) scheme has been presented. In this approach, the method classifies the service and for each service, the method generates different key set according to the attributes accessed. The method selects the keys in a randomized approach and chooses the keys at different time session. Generated key has been used to perform encryption or decryption where the schemes of encryption also selected in a random manner. The proposed MARK-SLE algorithm improves the security performance than previous SLABEalgorithm. Third, a Service Level Scheduler Based Encryption (SLSBE) Scheme is presented. In this approach, the security in service level and scheduling strategy is considered. For each service available, the method maintains the set of attributes being accessed. For each level of service and attributes, the method uses different keys and encryption standards. At the reception of user request, the method identifies the service claimed and set of attributes.

Keywords: cloudenvironment, encryption keys, security performance, Service Level Attribute Based Encryption (SLABE), multi attribute randomized key Service Level Encryption, ServiceLevelSchedulerBasedEncryption.

1. Introduction

The increasing volume of data belongs data any organization challenges the maintenance and retrieval of data. In earlier days the organizations maintain the data in centralized manner, which restricts the access of data from single point? However, maintaining the data in specific location introduces different challenges in terms of single point failure, higher traffic and so on. While maintaining the data in centralized manner, the entire request generated has been handled by a specific server. The performance of the system is highly depending on the capacity, where the server can handle only limited number of requests. This affects the performance of the system with fewer throughputs. Also, the growing size and volume of data introduces higher space complexity which cannot be afforded by a singlesystem.

To improve the performance of data induction and retrieval, the distributed computing environment has been emerged. The distributed system allows the organizations to store their information's in multiple locations and can be accessed at any point of time. On the other side, to store huge volume of data, it requires high capacity storage mediums like super computers. It is not possible for the organizations to their information in such systems, which has higher storage capacity, as they are more costly. Not all the organizations are capable of affording such huge money to purchase such costly resources. This is where cloud computing comes.

One of the developments is cloud computing. The path in which systems are sent speaks of a genuine change of perspective [1]. According to National Establishment of Guidelines and Innovation [2], it is characterized as, "Cloud computing is a model for empowering pervasive, helpful, on interest system access to a common pool of

configurable computing resources (e.g., systems, servers, stockpiling, applications, and services) that can be quickly provisioned and discharged with negligible management exertion or service supplier connection." In particular, this cloud computing has a lot of interest in ubiquitous services, where everybody can reach PC services via the Internet. You can build a gadget that contains a little show, processor and RAM with cloud computing. No other devices, such as optional memory, are required. It reduces the range of our new gadgets for innovation. It also reduces our system's costs.

Cloud services contain various security services based on the cloud provider deliver the contents in software services, platform services, infrastructure services, data services, based on the number of services is about the type of resource to be accessed. The user would have different jobs or process to be done and to complete their task. They can choose their service type. On the other side, the users of the organizations would have approved to access different resources stored in the cloud environment. However the users are eligible to access the resources, not all of them are in narrow and allowed. The users are restricted to access certain resource only, and that can be enforced according to the user profile.

Various cloud services are as follows:

- PAAS (platform as aservice)

  Consider, a job set j, which has N number of job where each requires different platform to be executed. To complete the tasks, it is necessary to get the specific platform where it is provided by the cloud environment. The PaaS is the type of service which is capable of identifying the platform required and the service provider can identify the platform required for the job and identifies the service to perform the task.

- SaaS (SOFTWARE AS ASERVICE)

  The software services are one which is available in presentation level. However, the interface available to perform the task can be classified according to the platform in which it is going to work. So, the software services are identified and selected according to the platform and based on the requirement the SaaS is selected to be executed in the cloud environment.

- NaaS (NETWORK AS ASERVICE)

  The network services are provided in the network layer which can be used to perform network level service access.

- Daas (DATA AS ASERVICE)

The data base services are provided to perform different data base access.

- IaaS (INFRASTRUCTURE AS ASERVICE)

  Different organizations would require high complex infrastructure to execute their task. The organization with huge batch process would require high complex resource like series of processors which are capable of executing millions of instructions in fraction. The organizations cannot afford such huge amount and by providing the infrastructure services, the organizations can access such infrastructure to execute their task. However, to access the infrastructure from different platform, there are number of middleware are generated and provided for the support of cloud users.

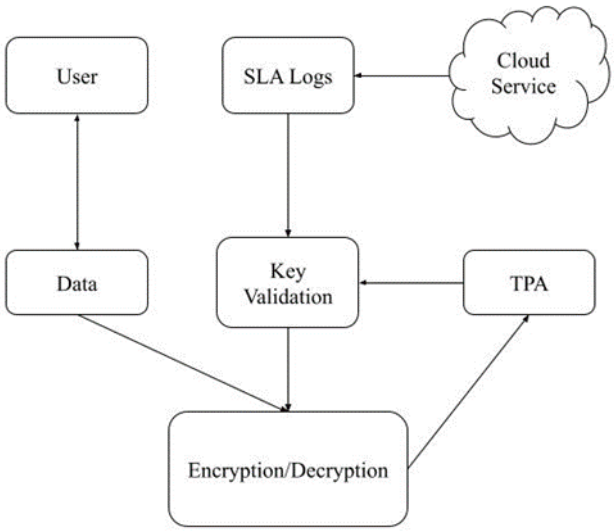

Figure 1: Cloud service crypto security

The data security is the major role behind the cloud environment because of the loosely coupled nature of the environment. The user of the environment does not know to service provider or resource provider. Service provider provides service which can be accessed by the legitimate users, but the third party auditor (TPA) is the responsible solve hand in verifying the identity of the user request the services. Figure 1 shows cloud crypto security. In general, the cloud security has been enforced by assigning public or private keys which can be tested on receiving any request. Such schemes are not suitable for the modern trend which can be spoofed easily. To improve the security performance, there is some methods have been proposed earlier. Some of the techniques use different encryption standards to store the data in the secure form. In that way, attribute-based encryption are used in private crypto security access. The method uses a different encryption algorithm for various attributes of the data. This would claim higher time complexity and reduces the throughput of the system. The resource of the cloud would be shared between different users of the system. Service provider takes responsibility to the provider or resource provider that the user accesses the correct data, not the malformed one. Providing such a factor on data has been named as public auditing [3].

Service oriented Operations:

The computational resources at different system stacks, such as SaaS, PaaS and IaaS, are supplied as pay as you go cloud services.

Cloud users only have to pay for what they used. 2) Cloud users have quickly access to elastic and scalable resources. Cloud users can launch more computing resources on time, release them at peak times and save their hardware/software capital expenditure to cope with job fluctuations. 3) The services are on-demand and can be configured themselves by cloud users. For cloud users, this makes it extremely convenient to access cloud services because they no longer need to interact and go through usually lengthy processing routines. 4) The Internet makes cloud services accessible. Cloud users are able to launch these services on any web-based platform. 5) Cloud users have access to computing services that are pooled and delivered to them regardless of their venue. Apart from these important characteristics, Cloud Computing often has multi-tenant architecture, which means that applications from multiple customers may operate or co-exist on the same physical unit. Cloud Computing is classified as Public Cloud, Private Cloud, Hybrid Cloud, and Community Cloud based on its ownership and technological architecture. Public Clouds provide services to the general public over the Internet, while a Private Cloud is dedicated to a single company or organisation. Hybrid Clouds integrate public cloud as well as private cloud models for specific business and technology requirements. Community clouds are normally used by similar purpose organisations.

Paper organized as follows: Section II describes related work carried out by related works. Section III presents overall proposed model architecture. Section IV discusses about overall performance analysis and comparison. Section V concludes followed with references.

2. Related Works

Problem of data encryption in cloud is reviewed and numbers of approaches are listed in this section. An authentication protocol is designed towards secure data transmission where data has been encrypted [4]. Also, allows the resource to be accessed through web browser. Multi level coding based data security is enforced in [5], where the method performDNA encryption and uses AES algorithm in encoding the data.Homomorphic

algorithms in encryption are more efficient has been enforced in [6], where the method use single bit with RSA algorithm to perform data encryption towards various attacks. A three bit level encryption techniques are presented where different data has been encrypted with various size of bits like 256, 192 and 128 bits [7]. Away from standard data protection schemes, to improve the performance of encryption, compression and steganography schemes an efficient approach is presented in [8]. The performance of various security schemes are analyzed and compared with the performance of RSA, MD5 and SHA1 approaches [9]. A combined approach is presented in [10], which clubs Byte rotation and ABE schemes to improve performance in peer to peer networks. Similarly, in [11], the proxy re-encryption and key aggregate schemes are clubbed to enhance security. In [12], author presents a retrieval approach on cipher text from huge data volume. The data are indexed using porter stemming and blowfish approach is used to encrypt the data where ECC is used for key generation and access restriction. A combined approach of erasure code with proxy re encryption to improve the security performance in data retrieval and data sharing is presented in [13]. Similarly, EncryScation is presented in [14], which is a secure encryption technique, which is used to authenticate user as well as obfuscation in server side.Cloud infrastructure provides various service trust models to incorporate the privacy controls on centralized data storage [15]. Specifically, trust strategy offers the confidential data level, but the reliability of data doesn't possess the services to quantify the degree of sensitive issues. The cloud service provides differential data compromise due to the failure of proper service maintenance to the user had security problems. Due to lack of information in centralized storage vast of info need a secure framework for big data information [16]. The clouds service provider (CSP) contains the minimal of security in network providers who want to access the data. All the access controls only maintained by administration of cloud content service provider. The data grids represent the smart information transformation (SIT) framework to secure the data in the form of a hierarchical structure. The represented big data management contains irregular auditing policy in intelligent grids [17]. Smart computing provides the different services to maintain the security. Specifically, the service level attributes based cryptologic ensures the type of service based security allotment to the requester. The lossless security in a cloud environment provides end to end security policy to meet the requirements for security policy [18]. The verifiability in outsourcing doesn't auditing the key system to verify authentication. This problem mainly occurred in the wireless network directly communicate the request through the centralized server without any auditing. The cloud agent providers access the data services security to obtain the protocols by inter cloud representation [19]. The adaptive concession rate (ACR) and minimal sufficient concession (MSC) both the method are to negotiate the security rule [20]. The cloud representation depends on the time factor evaluation of service providence based on the concession. The network and integrity system enhance the protocolstandards in service selection using business plan strategy. The enterprise resource planning (ERP) request the cloud vendors to distribute the data sources with security sharing mechanisms [21]. The successful fact of cloud provides the service in an outsourcing environment. The effects take place in service level security needs key security policy. The encryption at in different standards by choosing the service level in a cloud. The cryptographic security uses the secure dynamic auditing protocol framework to protect the cloud storage system [22]. The service which is directly accessed by the owner's permission to get the data. The multi-cloud environment uses the encryption services based on public key cryptographic techniques [23].To extend the cloud auditing framework with the support of the group key management system (GKM). This creates more time relevant access issues in the time of request and response state. Mostly data storage secured by key policy of dynamic auditing [24]. The data owners store the data and key in different format which is from encrypted format. The independent auditing resembles the key security to make verification through auditing clearance [25].cloud computing make potential task for handled multiple verification make vulnerabilities of unwanted authentication [26]. Cloud computing requires the owner trust level to specify the proof of key validation. The crypto policy fails this form of authentication access [27]. The multi authorized content doesn’t related the trusted authority verification to quantizing the theory of service from cloud provider [28].the cloud service selection doesn’t manage the complexity of data providence on different level based on the user preferences and functionality demands [29].

3. Problem statement

There are number of problems have been identified from the review and they are listed as follows:

- The public key private key based algorithm suffer with higher data leakage and produces poor throughputperformance.
- The profile based approaches uses different profile in encrypting different data and suffer with poor security performance.
- The existing methods suffer with higher overhead in key distribution and time complexity.
- The accuracy and efficiency of data security and access restriction isless.

- The time complexity and false ratio arehigher.

4. Objectives and Motivation of the research

The scope of the work is to design efficient data security algorithm which should consider the following facts:

- To improve the performance of securitylevel.
- To design efficient data security algorithm which should use different schemes for different services and the ABE should be adapted at servicelevel.
- The method has to adapt the attribute based encryption in servicelevel.
- The method has to classify the attributes in service level and the encryption standard has to be adaptedaccordingly.
- The method should select the keys in a dynamic way according to randomization technique.
- The method has to increase the public auditingperformance.
- The time complexity must bereduced.

5. Research Methodology

The center of this research is to give security to the cloud resources for secure data stockpiling in clouds that backings unknown validation. The proposed plan is utilized for open auditability and data reliance. An author whose attributes and keys have been denied can't compose back stale information. Conveyed access control of data put away in cloud so thatexclusive approved users with substantial attributes can get tothem. Verification of users who store and adjust their data onthe cloud. The personality of the user is shielded from the cloud amid validation. The engineering is decentralized, implying that there can be a few KDCs for key management. As indicated by our plan a user can make adocument and store it safely in the cloud. This plan comprisesof utilization of the three conventions are Service LevelAttribute Based Encryption (SLABE), Access Freedom andData Audit Management.

The service level attribute encryption (SLAE) performs identification of the nature of service and the level of service like (Software, platform, data, and infrastructure). The method classifies the attributes of the environment as sensitive and non-sensitive based on that an encryption method is chosen. For sensitive characteristics, the process selects a hash function which verifies the identity of a user with the help of TPA (Third party Auditor) and once the identity verification gets cleared then the access clearance is computed. When the user request explains both the service is fulfilled, and the sensitive values are encrypted using the specific key which could be decrypted by the user. For non-sensitive attributes, the method uses a public key based encryption which can be decrypted by user.

The Service Level Scheduler Based Encryption method is to minimize the time consumption for servers by used on automatic server consolidation strategy while guaranteed and transferred service level attribute. Current approaches for safeguarding confidential cloud data based on the encryption attribute. In these approaches, schemes vary in approaches and models, in order to detection and avoid false cloud data, the Service Level Scheduler Based Encryption (SLSBE) models proposed were studied. The principle of detecting the false without dropping legitimate packages was observed in all the proposals.

The most problematic elements of encryption are the protection of data in standardised time of key verification with the separate key of public key safety. To address the problem, cloud data protection standard based on session time key verification and using Service Level Verifiable Attribute-Based Encryption (SLVAE) was developed. To boost data protection, the proposed framework incorporates exponential max trust random encryption. Using the service level auditing protocol, the session time preserves the data with additional key verification n session requests to boost the public key generation. The session key is inserted in the data stored in a single storage by a third party. In a centralised cloud environment, this system enhances on-time safe verification using public key cryptography security system with the right factor of dynamic auditing protocol.

The presences of malicious users and adversaries temper the security walls and introduce different threats to the cloud environment. However, there exist numbers of techniques in mitigating such threats but could not perform that successful ratio. To improve the performance, an polynomial service centric multi model data encryption (PSCMM) technique is presented in this article. Instead of using same set of techniques and keys in data encryption, the novel technique use different standards and key sets for various type of services. The selection of scheme and key has been performed according to the polynomial operation. For any service request, a polynomial operation has been performed to decide the key and scheme has to be used. According to the result of polynomial function, the method performs data encryption, where the same is used to perform key selection

and method towards encrypting each attributes. This dual model encryption supports the performance development of data security in cloud. The proposed PSCMM algorithm has produced higher security performance with least tampering ratio.

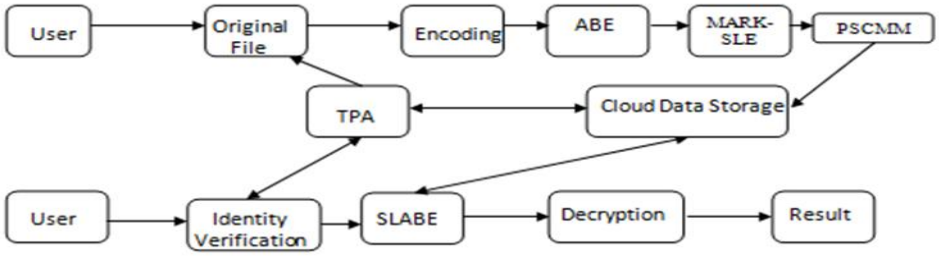

Figure 2: Overall Architecture Diagram

MULTI ATTRIBUTE RANDOMIZED KEY BASED SERVICE LEVEL ENCRYPTION APPROACH (MARK-SLE):

The architecture of multi attribute randomized key based service level encryption approach (MARK-SLE)and shows the functional components in detail. Data requesting conveying and sharing is a standout amongst the most generally utilized services in cloud figuring and prerequisite of information security develops with cloud processing spreading. Attribute-based encryption is one of the most alluring approaches to oversee and control file sharing in a cloud with its exceptional attribute registering properties. In this work, a novel multi attribute randomized key service selection to secure file sharing plan because of attribute control is displayed. The outline verifies the authentication in the cloud file framework with attribute-based encryption. This produces an efficient meaning of attribute figuring in cloud figuring condition. Given definition, safe and functional attribute-based encryption conspire without pairings under cloud processing situations was outlined. As per our examination and test, combine is picked plaintext secure in particular ID demonstrate and can fulfill file sharing application in cloud registering.

In this stage, the method identifies the list of attribute the being accessed by the service and classifies according to the Metadata. Based on the class of the service and the data, the method sorts the data as sensitive and non-sensitive. According to the class of data, the method selects the encryption standard and encrypts the data. Before that the user identity is verified using the third party auditor and data is encrypted accordingly.

Algorithm:

Input: Service Sr

Output: Encrypted Data Ed.

Start

Step: 1 Read service list Sl.

Step 2 Identify the list of attributes of Al.

Al = ∑▒Attributes∂Sr

For each attribute Ai

If Ai.class == Sensitive

Choose encryption algorithm

Ed= Encrypt data

Else

Step 3 Choose Encryption algorithm

Ed = Perform Encryption

End

End

Step 4 Return Ed.

Stop.

The above algorithm performs encryption selection according to the class of data and service that to select from the service list to provide the security.

Service Level Attribute Based Encryption (SLABE)Scheme

The SLABE performs recognizable proof of nature of service and the level of service like (Software, stage, data and framework). The technique arranges the attributes of the environment as delicate and non-touchy in light of that an encryption strategy is picked. In ABE system users might be shot of exchange decoding keys to unapproved users. To keep away from this pernicious key dispersion SLABE plan is utilized. It is additionally used to conceal user‟s attributes from the cloud and the users. Following is accomplished for figure writings to maintain a strategic distance from the pernicious key circulation. In these plan following is all the more difficult one. To enhance this key arrangement attribute based encryption (KPABE), it creates the misuse free attribute based encryption. Here n-bits user character spaces are characterized. Every piece speaks to the attributes. For following every attribute users has the extraordinary character. These character and user‟s attributes are avoiding users. Through this can't take in anything from figure writings about attributes coordinating or bungling. Attributes are named concealed typical attributes (HN) and shrouded character attributes (Stowed away).

A Setup key: This stage yields people in general key and expert key.

B Encryption: Encode message M with arrangement of attributes X, however attributes are Xhide covered up.

C Key era: Key era should be possible by access structure as info and produces yield.

D Decryption: Decoding should be possible with unscrambling keys for every attributes of users.

Above SLABE system is utilized to conceal attributes from approved and unapproved persons.

However, Key arrangement Attribute based Encryption (KP-ABE) is one of the types of ABE systems used here. The KP-ABE system's power can only be used to set the access structure's approaches. Since the approaches are the only thing in KP-keys. ABE's Here, the data owner believes in his or her own strength.

For touchy attributes the strategy picks a hash capacity which confirms the character of user with the assistance of TPA (Third party Auditor) and once thepersonality confirmation gets cleared then the access leeway is registered. At the point when the user demand clears both the service is satisfied and the touchy qualities are encodedutilizing the particular key which could be unscrambled by theuser. For non-delicate attributes the technique utilizes an openkey based encryption which can be unscrambled by the user.

Service Level Scheduler Based Encryption (SLSBE):

The Service level Scheduler Based Encryption (SLSBE) reflector cloud used to detect the cloud traffic and avoid the attackers. In these reflectors is using the Induction Detection System to rectify the road traffic to transmission data in the specific cloud servers. The indicator cloud is used to distribution data in cloud security consume to incidence in data cloud. In this cloud used to two reflector cloud one is Induction Detection System reflector Loader and another one is reflector cloud Router Reflector is used to rectify the traffic cloud and to transfer the data in the specific cloud servers. To initialise array permutation “S”, cloud scheduling technique is utilized. In key number of bytes is defined as “Length” which has range $1 \leq \text{length} \leq 256$ between 5 and 16, based on key length of 40 – 128 bits. The array "S" is first set up with the identity permutation. S is then processed for 256 iterations in the same way as the main PRGA, but with the addition of bytes from the key.

For I from 0 to 255

S[i]:= i

End for

J: = 0

For I from 0 to 255

j := (j + S[i] + key[imodcloud scheduler]) mod 256

Exchange values of S[i] and S[j]

End for

By enabling data verification and data correction in form of encryption standards helps to enhance data security in cloud environment. Public auditing can be enforced in several ways by maintaining the identity and verifying the user identity before modifying the data. In the data level, the data itself can be encrypted and stored, which can be decrypted in correct form by the user who has the exact decryption key.

Service Level Verifiable Attribute-Based Encryption (SLVAE):

In SLVAE, based on session time key verification for securing data in cloud data. Figure 3 shows implementation of proposed system. Using RSA based signature method, stored file data security is monitored. It is based upon concept of session time key verification model. Session time security is a challenge and response for on-time secured validation provide true authenticity. In client using on-time validation crypto policy techniques poses a challenge to cloud server and gets proof for challenge. Service-based session time verifies the security on time validation key that is stored in the remote server and proof is the value generated for the selected subset of file blocks. The client verifies the proof on session request time that it received from the server and the authentication is verified by TPAthe following are the key aspects,

• Due to dynamic measurement, service essence cloud computing models have no fixed infrastructure and security boundaries for all kinds of applications and data on cloud platform due to location transparency specializations. If a security gap occurs, it is difficult to isolate a particular body resource that has a threat or is left out.

• Cloud computing service delivery models, cloud-based services for based resources may be obtained through multiple providers. If there is a conflict of interest, it is difficult to find a united defense operation

• Unlocking user data for other unauthorized users, as open and accessible to the imagined resources of the cloud and multiple tenants.

In this stage, the service level is chosen by the data owner after the session time security integration the data is ready to encrypt. User data is secured with service level public key and can only be understood by serve chosen private key associated with that gnu data. This is followed by the time-frame of the session-generated data based on the update of the session. This implementation provides the service level key to verify the public keys based on maximization of numbers in prime layer element by multiplying mathematical formulas and numbers. It uses plain text or glossy texts and uses num-size block size data between 0 and 1 with some n values. More modules are encoded in the simplified process here, and each block should be less than the number (b) of the binary value. Session time encryption is the multiplication phenomenon, which means that the resulting effect that the plain text product will find is to multiply the gnome text ticker texts in the output.

SLVAE on time security

Input: preprocessed data Ps, Exponential session time ET

Output: output encrypted text

start

step 1. two exponential prime numbers P and Q is used to generate max confidence

Step 2 process the session based data encrypt using two-factor key

If (the prime factor p ≠ qsuch that. p & q)→key factor

{

Generate on time session key →Sk

Compute n= p × q;

}end if

Step 3. Calculate the intensity of data

If (d(n) = (p-1) (q-1).) factors of exp value e

{

The exponential integer value be chosen 1<e→Ps as e

User A possess the message m to encrypt B→A

Whether A be message decrypts, the authentication followed to user BUserA attained to Get the secure level public keys (nA, eA).

Update on session T→Ps

}

Step 4. compute the terms message at the regular interval [0, nA − 1].

Select a random integer k , 1 < k <nA, such that gcd(k, nA)) = 1.

if (c1 = k eA mod nA.) and (c2 = meA k mod nA)

{

Transfer the encrypted message request to user A as (c1,c2).

Return on state session T

}

End if

End if

Stop

Polynomial service centric multi model data encryption (PSCMM):

The proposed polynomial service centric multi model method maintains taxonomy of services which contains list of users allowed for each service at its property. Similarly, the data attributes are maintained in data taxonomy. Using these two, the service restriction is performed. On the other side, the method maintains, list of keys, schemes and key taxonomy. Using all these sets, the method performs polynomial data encryption towards data security development. Using the service and data taxonomy, the access restriction is performed. Similarly, using the different key set, scheme set, the method performs data encryption. The data encryption is performed in this model in two ways. This one is the primary level where each data attribute has been encrypted according to the polynomial function results. The polynomial function maintains a set of keys and schemes. It first identifies the list of attributes available in any data. For each data attribute, the polynomial function selects a unique random number according to the size of key and scheme set. According to the key and scheme selected, the method encrypts the data attribute. With the data attribute encrypted, the method adds the index of both key and scheme inform of encrypted text using the common key given. All the data attributes with the key blocks are added to the single data and given to the user. Each block has been given with same size which is used to identify the exact block in the decryption phase.

Polynomial ABSLDE (Attribute-Based-Service Level Decryption)

In this stage, the method first receives the encrypted text and extracts the last four bits. From extracted four bits, the method identifies index of scheme as well as key indexes. Using these two, method performs decryption to obtain the result generated by the PABE (polynomial attribute based encryption). Second, the data has been split into equal number of blocks according to the size. For each block, the method extracts the four bytes and identifies the index of key and scheme. Using them it has been decrypted to generate original data. All the block data obtained in decryption has been merged to produce original result.

PABSLE Algorithm

Given: Key set Ks, Scheme Set Ss, Encrypted Data Ed

Output: Original Data OD

Start

Read ks, ss, Ed.

KSindex = Extract four bytes from Ed.

Identify index of scheme si = Ascii(Ksindex(3,4))

Identify index of key Ki = Ascii(Ksindex(1,2))

Obtain first level original data Flod = Decrypt(Ed(1,(size(Ed)-4)),Ss(si),Ks(ki))

Split the data into number of blocks.

Data block db = size(Flod)Split(Flod,k)i=1 (8)

Here the value of K is obtained through secure channel or it has been fixed for number of time session.

For each block b

Identify the key index and scheme index as follows:

Si = Ascii(db(i)(last two bytes))

Ki = Ascii(db(i)(last before two bytes))

Original data Od = Decrypt(db(i),ks(ki), ss(si))

End

Merge all block decrypted text and produce result.

Stop

The working principle of the proposed polynomial attribute based service level decryption algorithm is presented. The method receive the cipher text and identifies the service level key and scheme using the last four byte values. Using them, the first level data is identified. Further, the data has been split into number of blocks of equal size and for each of them it identifies scheme as well as key indexes. Using them method performs decryption to produce result to the user.

6. Performance Analysis

The proposed methods on data security in cloud has been implemented as well as evaluated for their performance in several parameters. Methods are evaluated for tier performance on various simulation conditions. The results obtained has been presented in this section.

Parameter	Value
Number of Data Attributes	100
Number of Tasks	100
Number of Users	500
Number Services	50
Number of resources	20

Evaluation details used for problem of data security evaluation on different methods have been presented in Table 1. The evaluation results are presented in thissection.

Table2: Overall Performance

Parameters	Overall performance		
	100 Users	300 Users	500Users
Authentication	55	66	72
Security	69	74	81
False Classification Ratio	52	56	61
Time Complexity	71	76	82

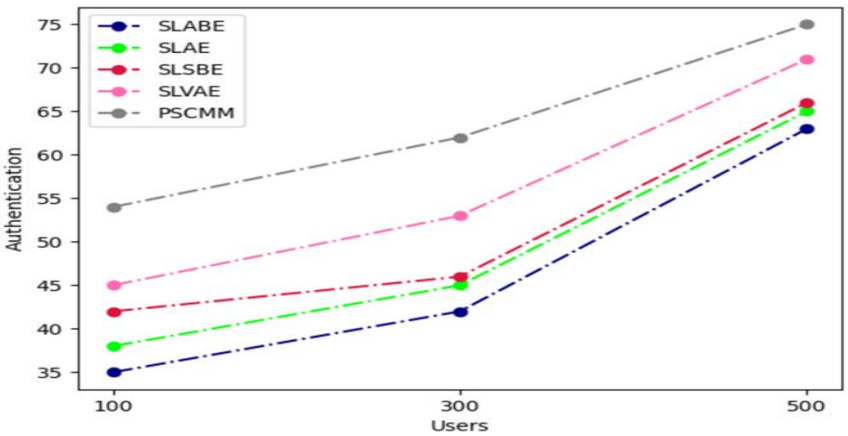

Figure 3: Overall Performance Analysis on Authentication

The authentication performance as shown in above figure-3produced by different algorithms are measured as well as compared with result of other methods. When compared with other techniques proposed method achieves better authentication performance.

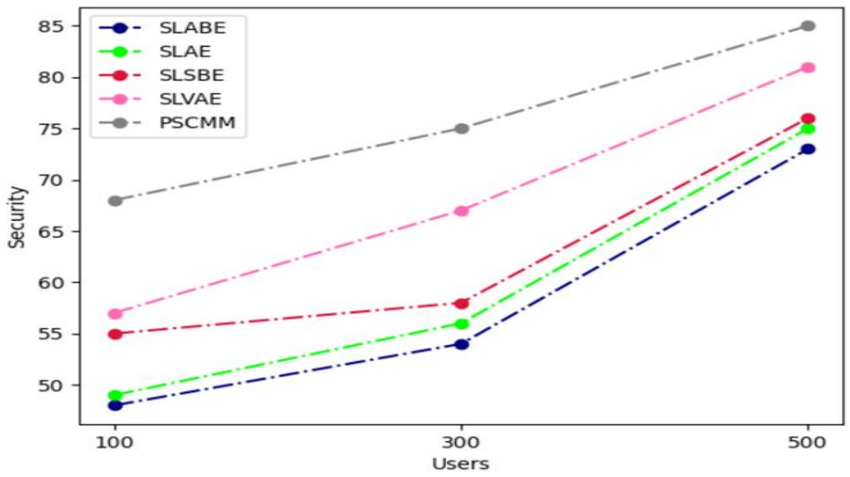

Figure 4: Overall security performance

The security performance as shown in above figure-4produced by various methods is measured as well as compared. When compared with other methods, proposed method achieves good security performance.

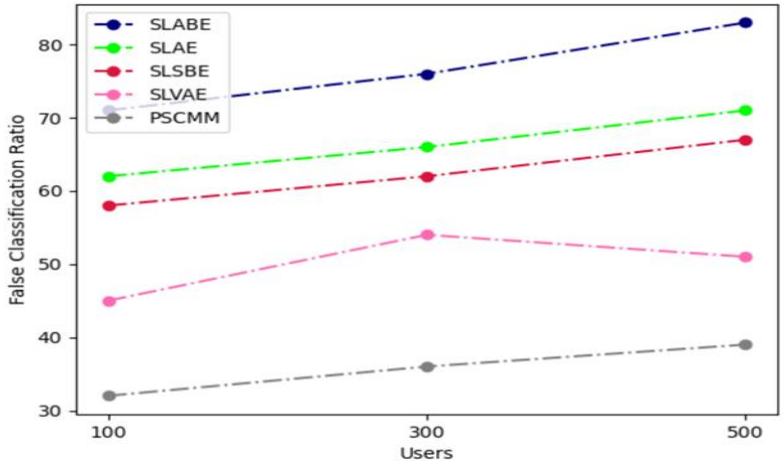

Figure 5: Overall false classification ratio

The ratio of false classification as shown in above figure-5is measured on different methods at different number of users conditions. The proposed algorithm have produced less false ratio compare to other algorithm.

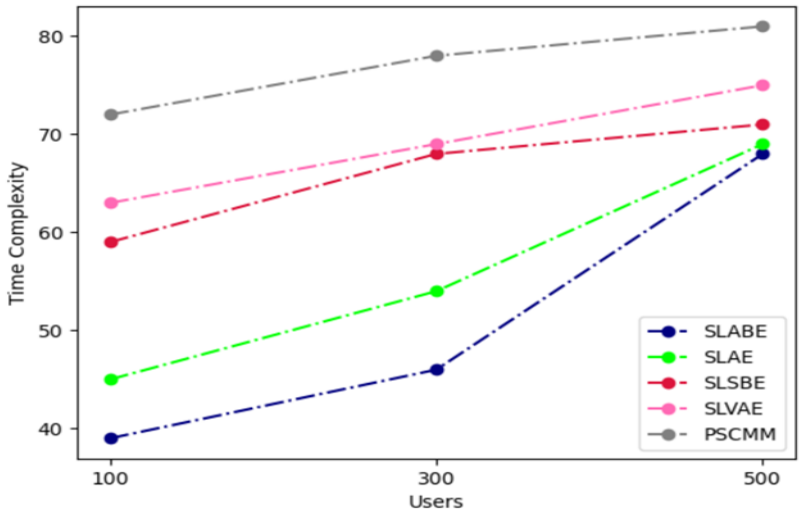

Figure 6: Overall time complexity performance

Time complexity as shown in above figure-6introduced by the methods have been measured as well as compared with result of other methods. When compared with other method proposed method achieves less time complexity.

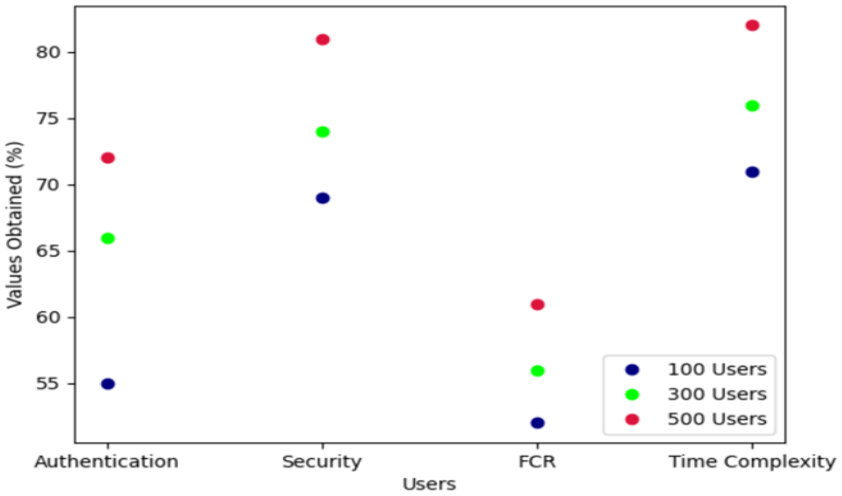

Figure 7: Overall parameter comparison

The above figure-7 shows overall parameter comparison based on the users.

7. Conclusion

Cloud computing is utilized as a part of a wide scale andtruly convey on its guaranteed advantages of versatility,scalability, flexibility, and economies of scale, the center of security needs to move towards concocting strategies toempower league of security capacities that are utilized today. For instance, organization of audit, personality management,verification, approval, and episode reaction should all be investigated in more prominent subtle element. This compares the encryption technique of multi model attributes. The method classifies the services and data as sensitive/ non-sensitive. Based on services and data, method selects the encryption to be used. Earlier the method estimates the access frequency and completeness to calculate trust of user. Based on the completeness measure the method allows or deny the user request.The single user can transfer the data cloud between the multi cloud servers. In this data to be deposited in the virtual cloud resource as well as to broadcast the information in service. The delivery can transport the data cloud in the scheduler in this scheduler to be provided to the network the deployment service. In this cloud server which cloud or network data to be relocatedrequire the path formerly only data must be removed. The positioning data should be transferred in the simulated infrastructure executive data should be relocated to the particular data cloud also proposed method improves the performance in public auditing false verification ratio is decreased up to 91% in cloud environment.Based on the services and data, the method selects the encryption to be used as similar way service acceptance for decryption whether the valid request at in session expired time. Based on the service session completeness measure the method allows or deny the user request.To achieve higher security performance, the method performs encryption in two levels. In the first level, the attribute based encryption is performed using polynomial algorithm which select different key and scheme for each attributes. In the second level, a service centric polynomial encryption is performed which select different key and scheme to encrypt entire data obtained in first stage. Finally, data has been given to user who can identify indexes of different key and scheme to obtain first level data which is further identified with the key and scheme to obtain the original data. With poor false ratio, proposed method achieves better performance in authentication and data security.

References

1. Daniel Ganzales, Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds, IEEE Transaction on cloud computing,vol. 8, issue 99, 2015.
2. JoosangBaek, “A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid”, IEEE Transaction on cloud computing, vol. 3, no.2, pp.233-244, 2014.
3. Baek, Q. Vu, A. Jones, S. Al Mulla, C. Yeun, “Smart-frame: A flexible scalable and secure information management framework for smart grids”, Proc. IEEE Int. Conf. Internet Technol. Secured Trans., pp. 668-673, 2012
4. G. Raj, R. C. Kesireddi and S. Gupta, “Enhancement of security mechanism for confidential data using AES-128, 192 and 256bit encryption in cloud”, IEEE (NGCT), pp. 374-378, 2015.
5. K. Rani and R. K. Sagar, “Enhanced data storage security in cloud environment using encryption, compression and splitting technique”, IEEE (TEL-NET), pp. 1-5, 2017.

6. Y. S. Gunjal, M. S. Gunjal and A. R. Tambe, "Hybrid Attribute Based Encryption and Customizable Authorization in Cloud Computing", IEEE (ICACCT), pp. 187-190, 2018.
7. W. Chen, "Efficient Key-Aggregate Proxy Re-Encryption for Secure Data Sharing in Clouds", IEEE (DSC), pp. 1-4, 2018.
8. S. Mudepalli, V. S. Rao and R. K. Kumar, "An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing", IEEE (ICICCS), pp. 267-271, 2017.
9. K. Rangasami and S. Vagdevi, "Comparative study of homomorphic encryption methods for secured data operations in cloud computing", IEEE (ICEECCOT), pp. 1-6, 2017.
10. R. Nivedhaa and J. J. Justus, "A Secure Erasure Cloud Storage System Using Advanced Encryption Standard Algorithm and Proxy Re-Encryption",IEEE (ICCSP), pp. 0755-0759, 2018.
11. M. Bouchaala, C. Ghazel and L. A. Saidane, "Revocable Sliced CipherText Policy Attribute Based Encryption Scheme in Cloud Computing", IEEE (IWCMC), pp. 1860-1865, 2019.
12. S. David, "A panoramic overview on fast encryption techniques for outsourced data in mobile cloud computing environment", IEEE (ICICI), pp. 476-480, 2017.
13. S. A. Oli and L. Arockiam, "Confidentiality Technique to Encrypt and Obfuscate Non-Numerical and Numerical Data to Enhance Security in Public Cloud Storage", IEEE (WCCCT), pp. 176-180, 2017.
14. Chauhan and J. Gupta, "A novel technique of cloud security based on hybrid encryption by Blowfish and MD5", IEEE (ISPCC), pp. 349-355, 2017.
15. R. Singh, Ataussamad and S. Prakash, "Privacy preserving in TPA for secure cloud by using encryption technique", IEEE (ICIIECS), pp. 1-5, 2017.
16. S. Belguith, "PU-ABE: Lightweight Attribute-Based Encryption Supporting Access Policy Update for Cloud Assisted IoT", IEEE (CLOUD), pp. 924-927, 2018.
17. D. Das, "Secure cloud computing algorithm using homomorphic encryption and multi-party computation", IEEE (ICOIN), pp. 391-396, 2018.
18. S. A. Khan, R. K. Aggarwal and S. Kulkarni, "Enhanced Homomorphic Encryption Scheme with PSO for Encryption of Cloud Data", IEEE (ICACCS), pp. 395-400, 2019.
19. K. Suthar and J. Patel, "EncryScation: A novel framework for cloud IaaS, DaaS security using encryption and Obfuscation techniques", IEEE (NUiCONE), pp. 1-5, 2015.
20. B. Jana, J. Poray, T. Mandal and M. Kule, "A multilevel encryption technique in cloud security", IEEE (CSNT), pp. 220-224, 2017.
21. G. Raj, R. C. Kesireddi and S. Gupta, "Enhancement of security mechanism for confidential data using AES-128, 192 and 256bit encryption in cloud", IEEE (NGCT), pp. 374-378, 2015.
22. K. K. Chennam, L. Muddana and R. K. Aluvalu, "Performance analysis of various encryption algorithms for usage in multistage encryption for securing data in cloud", IEEE (RTEICT), pp. 2030-2033, 2017.
23. S. Song, B. Choi and D. Kim, "Selective encryption and component-oriented deduplication for mobile cloud data computing", IEEE (ICNC), pp. 1-5, 2016.
24. Malik and B. Pandey, "Asymmetric encryption based secure and efficient data gathering technique in VANET", IEEE (ICCC-DS&E-C), pp. 369-372, 2017.
25. M. Marwan, A. Kartit and H. Ouahmane, "Applying homomorphic encryption for securing cloud database", IEEE (CiSt),pp. 658-664, 2016.
26. J. Shao, Y. Zhu and Q. Ji, "Efficient Decentralized Attribute-Based Encryption with Outsourced Computation for Mobile Cloud Computing", IEEE (ISPA/IUCC), pp. 417-422, 2017.
27. S. Alshehri, S. P. Radziszowski and R. K. Raj, "Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption", IEEE (ICDEW), pp. 143-146, 2012.
28. G. Lin, H. Hong and Z. Sun, "A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing", in IEEE Access, volume 5, pp. 9464-9475, 2017.
29. Reshma N.S, "A novel scheme for authenticated secured de-duplication with identity based encryption in cloud", IEEE (ICIS), pp. 228-232, 2016.