Multi Attribute Point of Randomized Key Service Level Attribute-based Encryption Standards for Secure Cloud Computing in Cloud Environment

S. Noordeen, K. Dinakaran

Abstract--- The growing size of information, security became the risk of access from centralized resource providers deploy them into the cloud, where authorized users could access them. To provide security to the cloud resources there are many service level agreements (SLA) are provided, but the problem of public auditability and data dependence is unresolved due to challenge in key auditing. The service level needs the security based on key auditing by choosing the different service level. To propose a multi-level attribute based randomized key auditing encryption service (MARK-SLE) to improve the service level of security in the cloud environment. Additional to third part key aggregate level with prime factor verification. Then compute the encryption and decryption of attributes accessed at each level to provide cloud security. Whatever the data modified by any user will be updated so that to provide data audit and data dependence by swapping the reference of address in the block modified. The method maintains user access history, where the user access details are stored. The access history is being used to make decisions on providing service to the user request. The proposed method increases the efficiency of public auditability and tampers resistance.

Index Terms: Cloud Computing, Data Security, Public Auditing, Service Level Encryption, Cloud Security.

1. INTRODUCTION

The cloud computing becomes the most leading environment in the modern information society. The organizations earlier maintain their data in a large distributed system or centralized server. The maintenance of data has leveraged their responsibility and cost higher. Also, the organizations forced to invest huge money in developing the environment. To solve this issue, the cloud environment has emerged which does not claim any responsibility for the organizations but costs little. The organizations maintain their data in the cloud and enable the user access through different services. The 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.

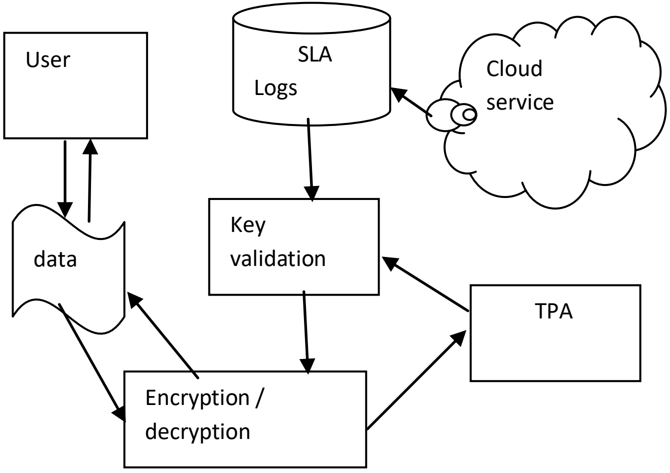


Figure 1: Cloud service crypto security

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 the service provider or the resource provider. The service provider provides the 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 the 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, the attribute-based encryption has been 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.

Revised Version Manuscript Received on 01 February, 2019.

S. Noordeen, Research Scholar, Bharathiar University, Coimbatore, Tamil Nadu.

Dr.K. Dinakaran, Professor and Head, Department of Computer Science and Engineering, PMR Engineering College, Maduravayal, Chennai, Tamil Nadu.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

By enabling the data verification and data correction in the form of encryption standards helps to improve the data security in the cloud environment. The 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.

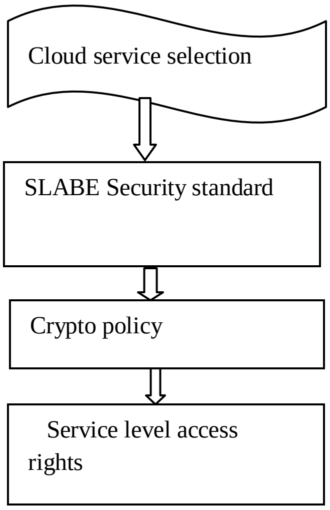


Figure 2: SLABE Multi-level security standard

The above figure 2 shows that the multilevel security standard service is providing from the cloud environment. Enforcing the data security in attribute level would produce good results but introduce higher time complexity. Still, such approaches suffer to achieve the required security level Agreement based Encryption (SLABE) due to the same method of selecting the encryption standard. To face advanced threats, the service provider must be well efficient in using the statistics of the user as well as the system. The service orient or service level encryption standard can be used to improve the performance of the cloud. The cloud would contain the number of services, but they can be classified into different categories and levels. For example, the user details verification services can be stacked in the top level, and the key verification services can be accumulated in the bottom. Similarly, the services can be stacked in different level according to their activity and importance. By enforcing different encryption standards for the different level of services, the problem of data security can be handled efficiently.

2. RELATED WORKS

There are some data security and public auditing schemes discussed and this section address some of them.

Cloud infrastructure provides various service trust models to incorporate the privacy controls on centralized data storage [1]. 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 [2]. 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 [3]. 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 [4, 5]. 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 [6]. The adaptive concession rate (ACR) and minimal sufficient concession (MSC) both the method are to negotiate the security rule [7]. 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 [8]. 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 [9]. 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 [10].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 [11]. 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 [12, 13].cloud computing make potential task for handled multiple verification make vulnerabilities of unwanted authentication [14]. Cloud computing requires the owner trust level to specify the proof of key validation. The crypto policy fails this form of authentication access [15]. The multi authorized content doesn’t related the trusted authority verification to quantizing the theory of service from cloud provider [16].the cloud service selection doesn’t manage the complexity of data providence on different level based on the user preferences and functionality demands [17].

This much reduce the performance of computing theory in more complex in nature of privacy and security.

All the methods have produced poor auditing performance and provide less security performance.

3. MULTI ATTRIBUTE BASED RANDOMIZED KEY SECURITY STANDARD

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 the user.

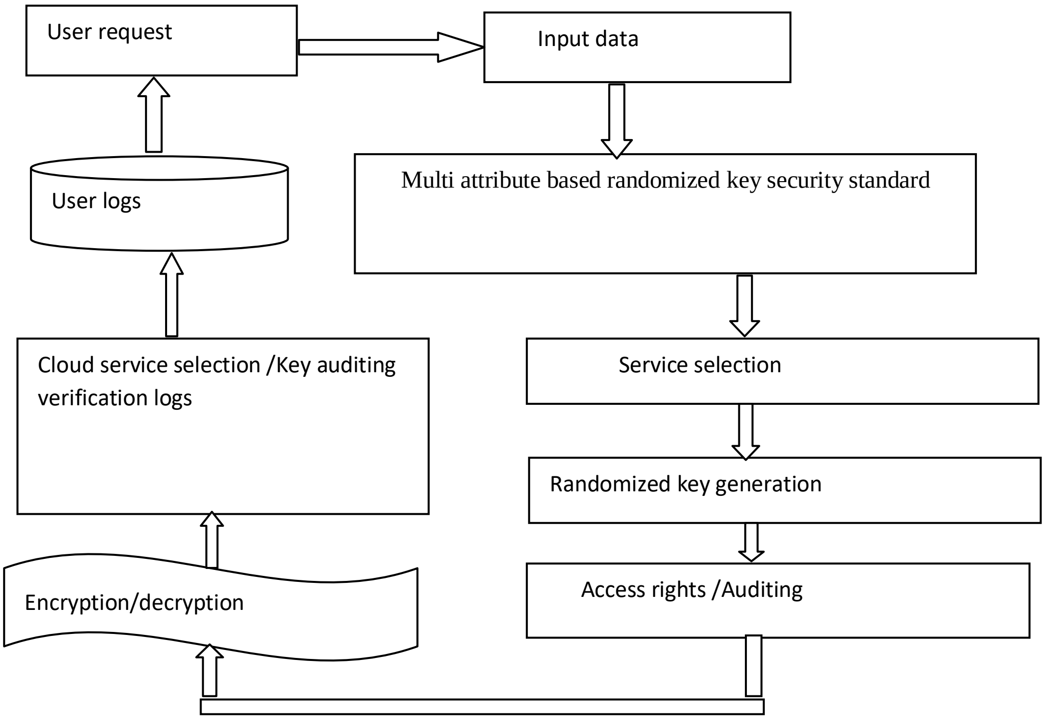

User request
Input data
Multi attribute based randomized key security standard
User logs
Cloud service selection /Key auditing verification logs
Service selection
Randomized key generation
Encryption/decryption
Access rights /Auditing

Figure 3: Architecture of Multi attribute service level based randomized key security standard

Figure 3, shows 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 the prerequisite of information security develops with the 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 the definition, we outline a safe and functional attribute-based encryption conspire without pairings under cloud processing situations. As per our examination and test, the combine is picked plaintext secure in particular ID demonstrate and can fulfill the file sharing application in cloud registering.

3.1 Service authentication request handling

The request generated by the user has been received, and the method identifies the list of services and their sub being needed to be accessed to complete the service request. Then for each level of service, the process determines the list of the attributes required to be obtained. Once the list of functions and attributes identified, the method performs access clearance. Based on the result the technique conducts service level attribute encryption. The generated results are used to produce results for the user.

```
Algorithm:
Input: User Request Ur.
Output: Null
Start
Step1 Read user request Ur.
        Identify the service claimed sc = Ur. Service
Step 2: Identify the list of services required SRl.
        SRL = $\sum Services\ \partial\ Sc.$
        For each service Si from SRL
Step 3: Identify the list of attributes.
                SA = $\int_{i=1}^{size(SRL)} \sum Attributes\ \partial\ SRL(i)$
Step 4 Perform Access Clearance.
                        If true then
                                Allow Access.
                                Perform service level ABE.
Perform data management.
```

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

```
            Else
                        Deny Access.
            End
Stop.
```

The above-discussed algorithm performs public auditing and verifies the trust of the user to allow or deny the user request.

3.2 Service level access clearance

The access clearance represents the trustworthy of a user in accessing the services. In this, a process to compute the level of approval the user maintained in obtaining the assistance from hisall-time record. The service records of the user in accessing the service are identified, and from the service record, we compute the overall frequency of service completeness. Based on the value of service completeness and its frequency the user will be allowed to access the service.

```
Algorithm:
Input: Access Log Al, Service List Sl.
Output: Boolean
Start
Step 1 Read service list Sl.
Step 2 Read access log, Al.
    For each service Si
        Compute frequency of access AFreq = $\frac{\sum Al(i).service==Si}{Total\ services\ accessed}$
Step 3 Compute service completeness measure SCM.
        Scm = $\frac{\sum Al(i).service==Si}{total\ services\ accessed} \times \frac{\sum Al(i).service==Si\ \&\&\ Al(i).status==completed}{size(Al(i).service==Si)}$
            If Scm> SC-Th
                    Return true
            Else
Step 4:     Return false
            End
    End
Stop
```

The above-discussed algorithm computes the service access frequency and completeness measure. Based on calculated measures the method returns the Boolean value.

3.3 Randomized key security standard

The effective providence uses the randomized key security using RanKeygen to setup phase, and key generation phase takes care of assembling the keys needed for the entire operation. The input to the key generation is a public key and secret key and the attribute S.

```
      Step 1: For each attribute type Ati from Nat
            Attribute length define sequence Rseq s
        Step 2 Compute the keygenKgen= $\int_{i=1}^{size(Nat)} \emptyset(Rks.Region, i)$
        Step 3 compute service selection based Select a random number R.
            Select random key Ek.
            E-key = $\int Cr(R)$
        Step 4  Add to key set ks.
            Ks = $\sum(Key \in Ks) \cup Ekey$
        End
```

Consider the R -→KeyEnc where a key is a data cyclic security key. The secret key will be generated with the input of the asymmetric key public key.

3.4 Multi attribute based service level encryption/decryption

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 = $\sum Attributes\ \partial\ Sr$
        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.

3.5 Data Audit Management

Whenever a data being modified or a block of information is modified, the method verifies the trustworthy of the user, and upon success, the block reference is altered to new recommendations. This takes effect in the other user immediately.

3.6 Secured authentication for request handler

The contribution to the decoding is a public key, randomized key, get to structure and private key. The client verifies the data with the private key. Consequently, the client can decode with the digital signature and private key. The private key matches with the mystery key and gets to structure. On the off chance that private key matches, at that point it will unscramble the hash work. Else it returns to the client. Here the unscrambling did by server specifically. Also, the decoded hash work R(Kgen) = K(x) information is checked. Here unscrambling is done straightforwardly by the server.

Although the outsourced unscrambling is financially savvy contrasted with the proposed calculation, it doesn't suites the constant frameworks as it has overheads regarding time. The general design depicts the well-ordered process. Initially, the client is confirmed with public society key related to the entrance structures.

4. RESULTS AND DISCUSSION

The proposed multi attribute randomized key based service level attribute encryption algorithm has been implemented and evaluated for its efficiency. This security framework was performed using Microsoft visual framework 4.5 using c#.net cloud simulator with back sql server for log maintenance performance of the algorithm has been measured in different measures. The method has produced efficient results in all the factors considered.

Table 1: Details of simulation parameters

Parameter	Value
Number of Services	100
Data type	Data files
Number of users	3000
Service provider	CSP

Table 1, shows the details of the simulation is used to evaluate the performance of the proposed algorithm. The public auditing efficiency evaluated by using the keygen policy of total key generated to verify correct access by submitting to valeted by third party auditor.

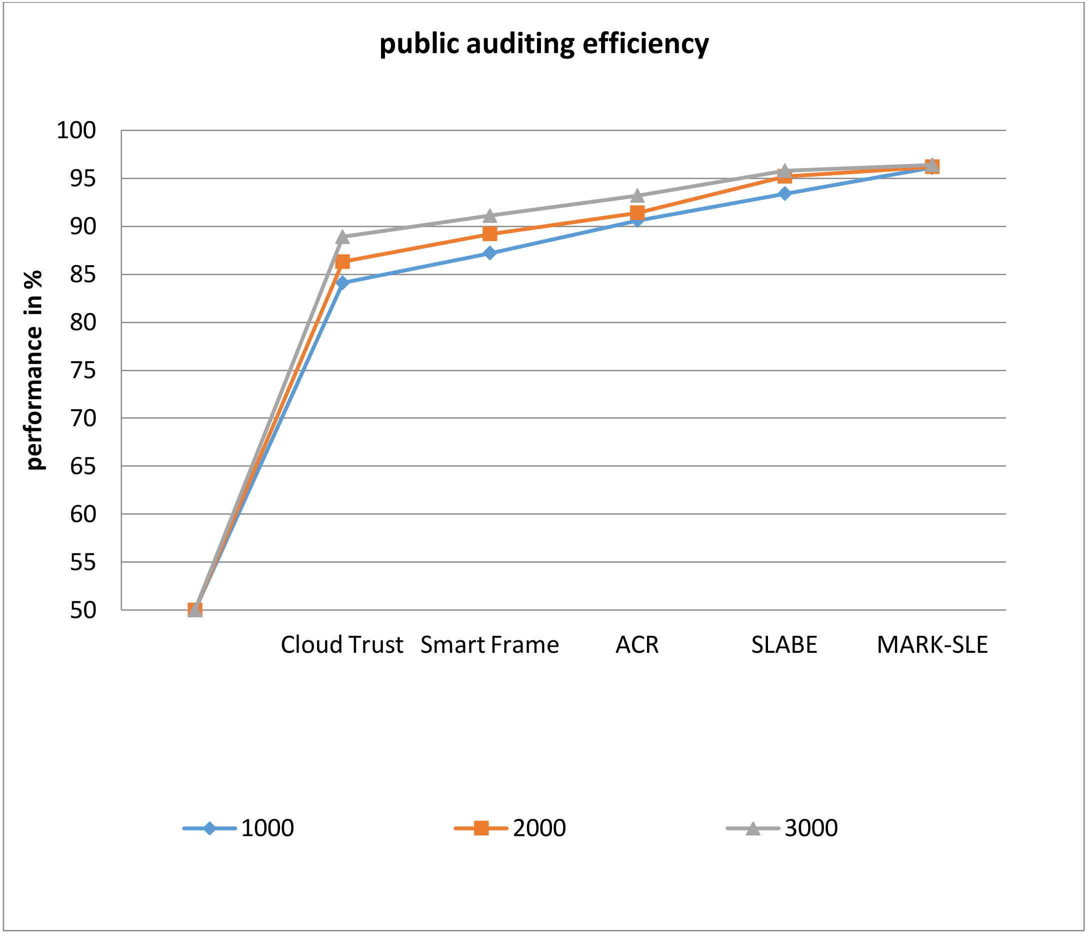
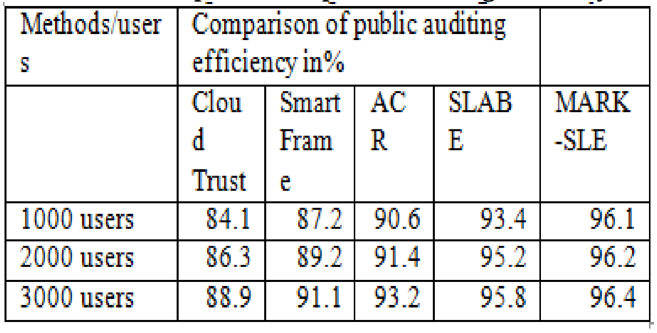


Figure 4: Comparison of public auditing efficiency

The above Figure 4, shows the comparison result on public auditing efficiency produced by different methods and it shows clearly that the proposed method has produced higher public auditing efficiency than other methods.

Table 2: Comparison on public auditing efficiency



Methods/users	Comparison of public auditing efficiency in%				
	Cloud Trust	Smart Frame	ACR	SLABE	MARK-SLE
1000 users	84.1	87.2	90.6	93.4	96.1
2000 users	86.3	89.2	91.4	95.2	96.2
3000 users	88.9	91.1	93.2	95.8	96.4

The above table 2 shows the comparison of public auditing efficiency with different methods the proposed system 96.1 % efficient than other compared methods. The throughput evaluation is overall performance of secured verification by right key of access given authenticator do by encryption and decryption to deliver the secured service.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

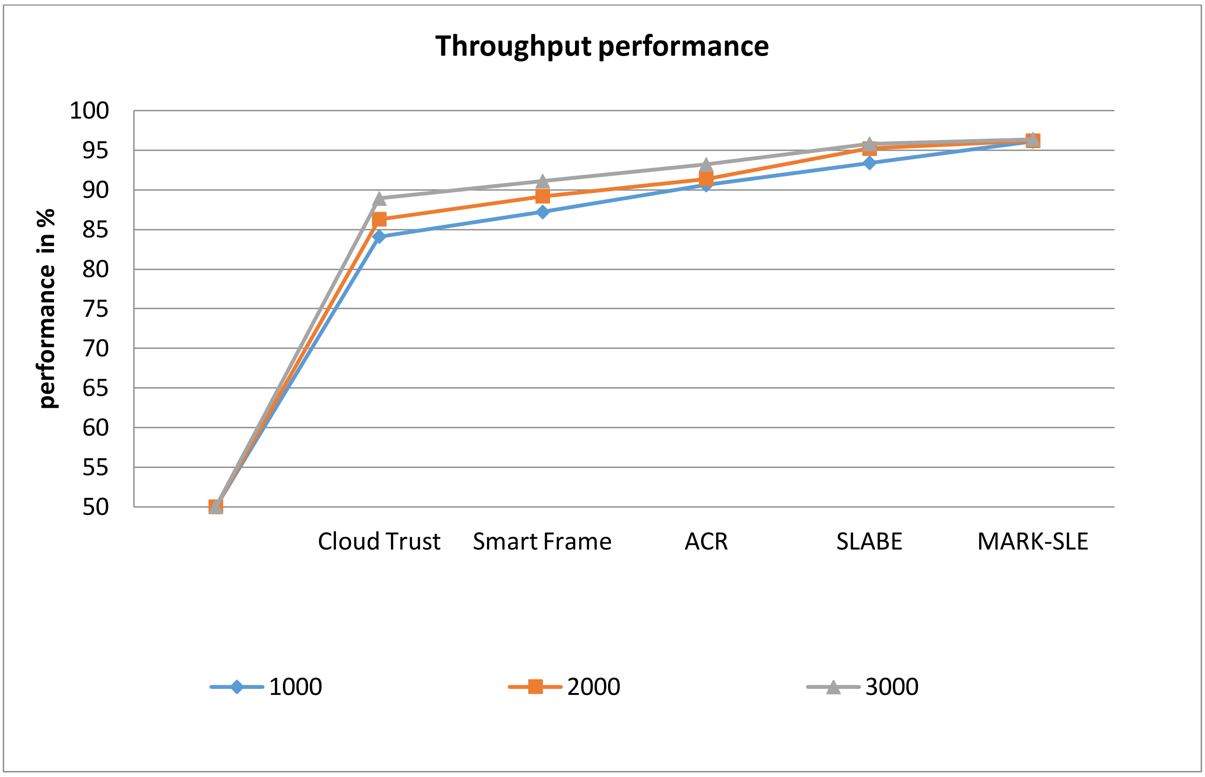


Figure 5: Comparison of throughput performance

The above Figure 5, shows the comparison of cloud service throughput performance produced by different methods and it shows clearly that the proposed method has produced higher throughput than other methods.

Table 3: Comparison of throughput performance

Methods/users	Comparison of throughput performance in %				
	Cloud Trust	Smart Frame	ACR	SLABE	MARK-SLE
1000 users	87.4	90.3	93.4	95.6	96.2
2000 users	91.7	92.1	94.2	95.7	96.4
3000 users	92.4	92.8	94.8	96.2	96.7

The cloud service throughput performance is shown in above table 3 with different methods the proposed system 96.2 % efficient than other compared methods. The comparison on throughput performance produced by different methods and it shows clearly that the proposed method has produced higher throughput than other methods. The time complexity is evaluated by total number of request to verify by the logs to access the data with the time of preference.

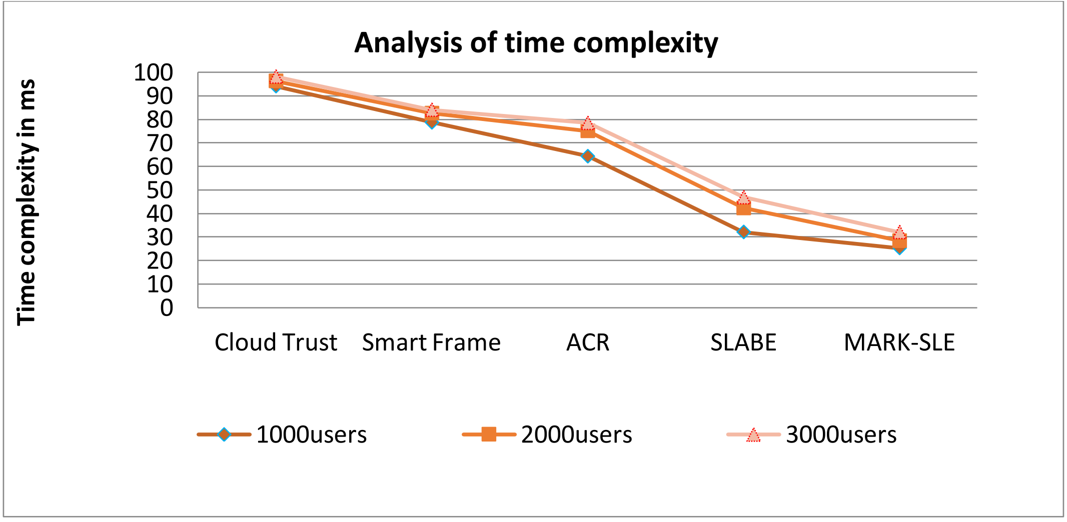


Figure 6: Comparison of time complexity

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The above Figure 6, shows the comparative result on time complexity produced by different methods and it shows clearly that the proposed method has produced less time complexity than other methods.

Table 4: Comparison of time complexity

Methods/users	Comparison of time complexity in Mille-seconds (ms)				
	Cloud Trust	**Smart Frame**	**ACR**	**SLABE**	**MARK-SLE**
1000 users	94.1	78.7	64.3	31.2	25.3
2000 users	96.3	82.6	75.1	42.3	28.4
3000 users	98.2	84.1	78.5	46.9	32.1

The above table 4 shows the Comparison of time complexity in Mille-seconds efficiency with dissimilar methods the proposed system 25.3 (ms) lower complexity efficient than other compared methods

5. CONCLUSION

In this work, an efficient Multi Attribute Randomized Key Service Level Encryption (MARK-SLE) is discussed. The method classifies the services and data as sensitive/ non-sensitive. Based on the services and data, the method selects the encryption to be used. Earlier the method estimates the access frequency and completeness to evaluate the trust of the user. Based on the completeness measure the method allows or deny the user request. The data encryption and public auditing are enforced in service level which increases the performance of public auditing as well 96.23 % well time complexity 25.3 milliseconds. The proposed method improves the performance in public auditing, throughput and reduces the time complexity as well.

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, issue 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. A. Bartoli, J. Hernandez Serrano, M. Soriano, M. Dohler, "Secure lossless aggregation for smart grid M2M networks", *Proc. IEEE Conf. Smart Grid Commun.*, pp. 333-338, 2010
5. Bartoli, J. Hernandez Serrano, M. Soriano, M. Dohler, "Secure lossless aggregation for smart grid M2M networks", *Proc. IEEE Conf. Smart Grid Commun.*, pp. 333-338, 2010.
6. C.-K. Chu, J. K. Liu, J. W. Wong, Y. Zhao, J. Zhou, "Privacy-preserving smart metering with regional statistics and personal inquiry services," *Proc. 8th ACM SIGSAC Symp. Inf. Comput. Commun. Soc.*, pp. 369-380, 2013.
7. KwangMongSim, Agent-Based Interactions and Economic Encounters in an Intelligent InterCloud, IEEE Transaction on cloud computing, vol. 3, issue 2, pp:358-371, 2015.
8. Shivamkupta, Moderating Effect of Compliance, Network, and Security on the Critical Success Factors in the Implementation of Cloud ERP, IEEE Transaction on cloud computing, vol.4, issue 4, pp:440-451, 2016.
9. Kan Yang, An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing, IEEE Tran., on parallel and distributed systems, vol.24, issue 9, pp:1711-1726, 2013.
10. C. Wang, K. Ren, W. Lou, J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," *IEEE Network*, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.
11. K. Yang, X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges Methods and Opportunities," *World Wide Web*, vol. 15, no. 4, pp. 409-428, 2012.
12. K. Ren, W. LouQ. Wang, C. Wang, J. Li, "Enabling Data Dynamics and Public Auditability for Storage Security in Cloud Computing," *IEEE Transaction. Parallel Distributed Systems*, vol. 22, no. 5, pp. 847-859, May 2011.
13. C. Wang, Q. Wang, K. Ren, W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," *Proc. IEEE INFOCOM*, pp. 525-533, 2010
14. Y. Zhu, H. Hu, G. Ahn, M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage," *IEEE Trans. Parallel and Distributed Systems*, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.
15. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, S.S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds," *Proc. ACM Symp. Applied Computing*, pp. 1550-1557, 2011.
16. Jesus Luna; Ahmed Taha; Ruben Trapero; Neeraj Suri Quantitative Reasoning about Cloud Security Using Service Level Agreements IEEE Transactions on Cloud Computing vol.5, pp 457 – 471, 2017
17. Yuli Yang; Rui Liu; Yongle Chen; Tong Li; Yi Tang Normal Cloud Model-Based Algorithm for Multi-Attribute Trusted Cloud Service Selection, IEEE transaction vol. 6, pp 37644 – 37652,2018.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication