RESEARCHERID
THOMSON REUTERS

[Noordeen, 6(4): April 2019]
DOI- 10.5281/zenodo.2639756

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

SERVICE LEVEL VERIFIABLE ATTRIBUTE-BASED ENCRYPTION USING SESSION TIME KEY VERIFICATION FOR IMPROVING THE CRYPTO-SECURITY IN CLOUD DATA MANAGEMENT

S. Noordeen[*1] & Dr.K. Dinakaran[2]

[*1]Research Scholar, Bharathiar University, Coimbatore, Tamil Nadu.

[2]Professor and Head, Department of Computer Science and Engineering, PMR Engineering College, Maduravayal, Chennai, Tamil Nadu

ABSTRACT

The day to development of internet communication, information security has a problem due to data leakage. So the security development in the centralized cloud environment needs advanced standards for protecting data, privacy, and key management. The most problematic factors which are the cryptography encryption is for protecting data with the separate key in public key security in standards time of key verification. To overcome the problem, we propose a cloud data security standard using Service Level Verifiable Attribute-Based Encryption (SLVAE) based on session time key verification for securing the data in cloud data.The proposed system integrates the exponential max confidence random encryption to improve the data security. The session time maintains the data with additional key verification n session request to improve the public key generation using the service level auditing protocol. The third party integrates the session key embedded in the data stored in a single storage. This system improves the on-time secured verification using the public key cryptography security system with the right factor of dynamic auditing protocol in a centralized cloud environment.

Keywords*: cloud security, public key cryptography, TPA, service level security, session time, service authentication.*

I. INTRODUCTION

Cloud computing process provides various services to secure the data from unauthorized access. This provides security against malware attackers, intruders, and crack finders and soon from the security issues. All the data in cloud management be centralized to open access the data. The services may be software, application, information, files, etc., All over the information in cloud data management be secured to protect the data. Due to the fact of attackers talents, the information is theft and read or modify the data. So data leakage is probability raise because of key leakage problems. The attackers get a chance from data transmission to create network mitigation to access the data. Most of the cloud servers protect the data using the crypto-defended database in remote access to give an authentication through the session validation time.

It moves the application software to remote data centers for large data centers that are stored by server systems. Important access to client data and stored on the remote server based on the session is verified. The customer then, through Internet access, can use data technology to change the data and save it. This service-level cloud computing technology has a number of challenging design issues, though it has been seen as a trusted service site, with security and performance concerns.

[Noordeen, 6(4): April 2019]
DOI- 10.5281/zenodo.2639756
ISSN 2348 – 8034
Impact Factor- 5.070

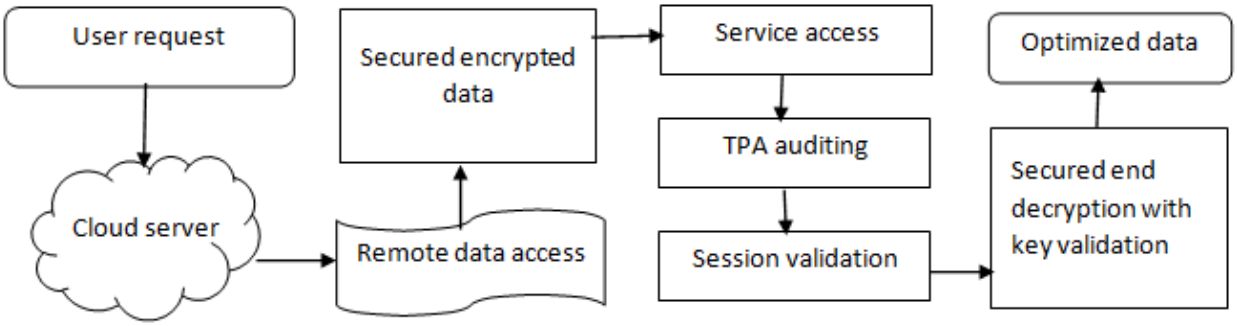

Figure 1 session based service level cryptographic security process

Security issues One of the biggest concerns is leak protection in session time checking. Figure 1 shows the session-based service level encryption security process saves untrusted server Troubleshooting access to remote data service. The problem is that there is no data integrity. For example, security service providers can decide to hide data using Crypto encoding to protect the service in a session verification service by a third party audit (TPA). As a result, the server data validation key can delete data request that the client does not require session verification without a time password (saving). Thus the customer must have the knowledge of remote data by monitoring the continuity of data stored contiguously.

Cryptography is a combination of data mathematical handling text changing (cryptosystem text) for both texts (key). Using the text conversion key is used on text with the ciphertext encoding protocol. And using the text algorithm to change the cursor text used on the spinning text. Before the encryption and removal algorithm, some algorithms must first be created in the core of the team. During encryption, there are three basic process-key generations, encryption and decryption process.

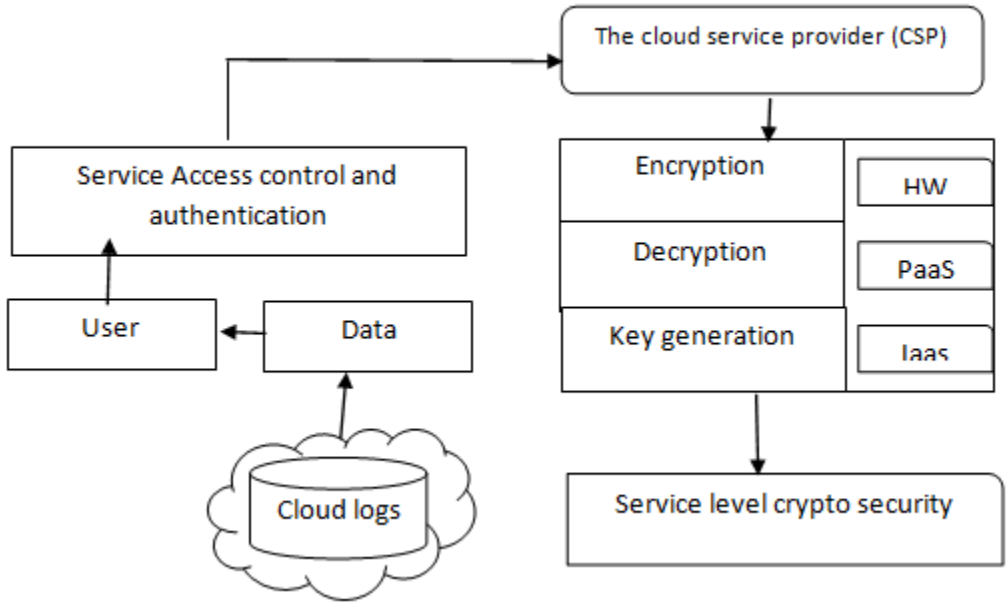

Figure 2: service access control in cloud security

[Noordeen, 6(4): April 2019] ISSN 2348 – 8034
DOI- 10.5281/zenodo.2639756 Impact Factor- 5.070

The data security is the primary role of protecting data in the cloud environment because the security is not sufficient to make data authentication. The user of the environment does not know to the service provider or the resource provider. Figure 2 shows the service access control in cloud security. The service provider provides the cryptographic service which can be accessed by the legitimate users, but the Third Party Auditor (TPA) is the single responsible hand in verifying the identity of the user request the services. In general, cloud security has been enforced by assigning public or private keys which can be tested on receiving any claim based on encryption and decryption. Such schemes are not suitable for the modern trend which can be spoofed easily. To improve the security performance there are some methods has been proposed earlier. Specifically auditing service level attribute-based encryption standards are mostly used.

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 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 some 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 during decryption and the essential 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 based on service level attribute for a different level of services, the problem of data security can be handled efficiently.

II. LITERATURE SURVEY

Most of the Traditional certified public key encryption use the signature-based verification methods [1]. Given authentication is a user's public key created randomly and are identifiable. Security is important therefore some trustworthy authority should have a certificate depending on the user's identity.

A signer depends the identity is expected to produce required privacy with a public key that he does not know the relevant private key in the real data before the key verification[2]. The common security against an intruder, such verification approach, is to interfere with the functional interference of the cryptographic system. However, the user’s are able to create part of their access rights to partial access with others requesters and make them more searchable for their records have initial authentication.

The Cloud is a terrible work specifically for users with tightly computed computing devices [3]. More and more users can use cloud storage as they do not care about the need to verify its integration. It is saving and unloading the universal data access load in independent geographical locations. At the same time, it expects capital from the cloud computing company, which costs more hardware [4], software, and employees maintenances, etc.

Many authorized cloud storage systems, where a number of officials are located, are a co-existent and efficient and accessible data access control plan co-existent and each power can provide free attributes [5]. Specifically, we propose common crypto aides Program to a Multiple Transitional Authority and apply it to the basic techniques to design the data access control program. Our attribute is canceled once the efficient way of securing both security and backward security

The cloud computing resembles the customer engagement by audit indicates that his information cloud is stored in cloud computing, [6] and can actually be in the reach of the economy, which is perfect. This is a significant step towards practicality since cloud computing services do not include archive or backup data, such as volume change, insertion, and deletion of data formats, general formats of data functions, and cloud computing services

The traditional security issues are still in the cloud computing environment. But as the definitions of Enterprise are extended up to the cloud [7], the traditional security mechanisms are no longer applicable to apps and data.

[Noordeen, 6(4): April 2019] ISSN 2348 – 8034
DOI- 10.5281/zenodo.2639756 Impact Factor- 5.070

Encryption schemes support encrypted queries on encoded data as proposed. But all of them have a significant loss of expensive data reclassification, single-user access or a shared set of secret keys [8, 9] depending on a set of keys among many users. Instead of maintaining a large tape library and arranging the vault (shop) to secure the data.

One can implement the performance efficiency of [10] and adjust the use of the problem by adjusting the short-term variation or verifying the integrity of, i.e.how are they determined for the dynamic auditing service Outbound storage to disclose the issue of changing adaptation by expanding the package set. Our audit service techniques [11] are structured based on updates supporting fragmentation, random sample, coding-hash table, outsourced data and proven timely disappearance. To fight the information leak, we have a zero-knowledge technique that converts data to the Integrity Testing [12]. This to show stock analysis and performance analysis as safe and efficient.

The main search technique in traditional and efficient simplicity is to use the data to retrieve data secrets is useless [14] Outsourcing [13], the data owner must be previously hidden. So the cryptography and efficiency of encryption cloud data is a very challenging task to design a more efficient design of how two objectives are encrypted.

In some cases, some proxy [15] is to represent the test work for remote data. However, some state information on proxy cloud storage servers [16] is notable because these PDP programs are not safe. In ordinary pre-plans, a proxy is a semi-reliable party model that is intended to be honestly done in the process of re-formatting. This means that we must put a relatively high level of trust in the representatives [17], before that, eg. Some applications may not be suitable for cloud-based file sharing systems.

New Public Key Encryption Methods that Produce Constant Sensory Books The Gear Books are the set of any set decryption rights capable group [18]. Attribute-based encryption (ABE) to protect users' identity. Abe is widely used in most of the [19] places, particularly in cloud computing. In this analysis, the equality test is to link the public key with the main principle of encryption. Cloud servers data crucial importance is that users, once cloud servers lose data control over their data, provide a simple, cost-effective, and flexible way to manage data [20].

Various issues due to complex nature on security as follows

1) The process of increasing the complex system leads the execution time. So the procedure should be simple to implement the structure fast to the data attackers.

2) Compared to the length of the key, it takes large size key, most of the method of execution provides the greater the speed of execution.

3) Depending on the selection of exponential logical operations used for any algorithm overall performance text, the key, and the cursor text. My algorithm, all these issues are considered to improve the performance of the encryption algorithm.

III. IMPLEMENTATION OF THE PROPOSED SYSTEM

Cloud is the most centralized security service on protecting data and service provider must still be concerned that request based data to the given the content. The most important cloud data among this privacy in a time-based schedule. This should be allowed to manage the level allowed to provide the key in the time intervalto protect the data and allow it to work through verification. Cloud clients require computational performance protection effect and maintain their data cloud providers are still in the process of increasing performance levels and to maintain data's own content to find various methods to formulate the data form and analysis on the crypto-security cloud Information and encryption, companies and the client of the cloud should be done Many of the cloud's point of view for others is a lack of interest for a variety of purposes, as the most important issue is the broader network of communications to exchange information. Therefore, we mainly focus on the security of information using the encryption and decryption algorithm of the cloud computing industry.

[Noordeen, 6(4): April 2019]
DOI- 10.5281/zenodo.2639756
ISSN 2348 – 8034
Impact Factor- 5.070

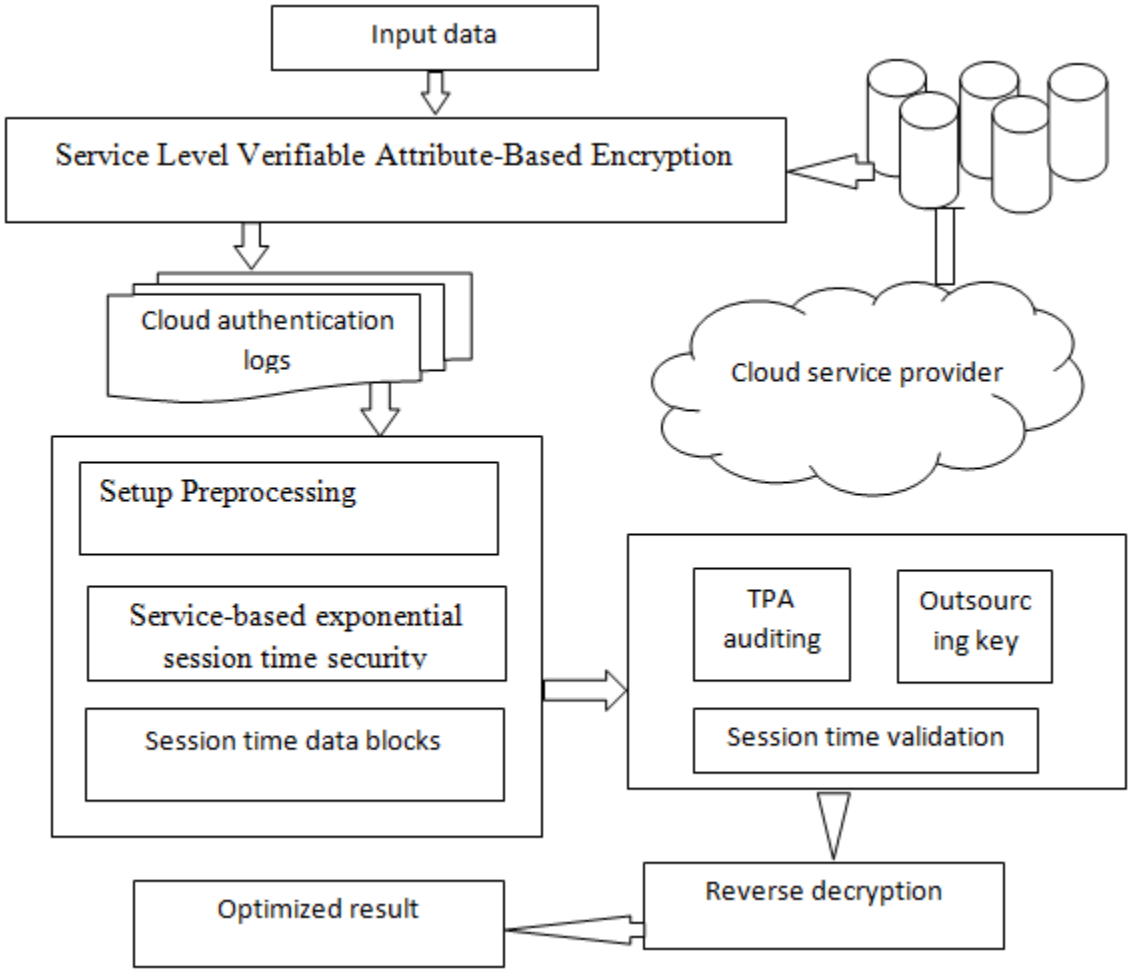

Figure 3 Architecture diagram for the proposed system

In the Service Level Verifiable Attribute-Based Encryption (SLVAE) based on session time key verification for securing the data in cloud data.Figure 3 shows the implementation of the proposed system. The security of the stored file data is continuously monitored using RSA based signature algorithm. It is based upon the concept of session time key verification model. The session time security is a challenge and response for on-time secured validation provide true authenticity. In the client using the on-time validation crypto policy techniques poses a challenge to the cloud server and gets the proof for the challenge. The 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 TPA.the 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.

[Noordeen, 6(4): April 2019] ISSN 2348 – 8034
DOI- 10.5281/zenodo.2639756 Impact Factor- 5.070

A) Key features of the proposed system

1. It depends on the domain and sets a special trusted agent on each service which is based on the request. Cloud resources cannot be managed in a trusted domain by a cloud provider.
2. The cloud provides different roles based on the group request or single request the security be varied at the level of service providers
3. It conducts the trust belief in organizations to believe that it is one of the kinds of service to step up.
4. Take the time factor and transactional factor into the account of confidence decision and renewal mechanisms.

3.1 Setup Preprocessing

The preprocess initialize data checks the data through verifiable outsource in the form of valid data. In this preprocessing stage setup up the cloud authentication request and response environment to provide the security. Further at initialization, the data checked by the originality without any noise and duplicated data. The huge level of instructed data is ordered to preprocess as recordsand to reduce the dimensionality of raw data. Henceforth, concerns regarding all the attribute are infill case or the data be to check it is empty or not. This verifies the non-structured data be a valid form of files of noise contained unstructured file be removed at in any other point noise-free data to process.

Algorithm: Service level set up preprocessing

```
Step 1: Input raw data Rd {rd1,rd2,…rdn};output :noise free data
        For each rd (record set← Rs)
            Check is Empty==NULL
                Fill attribute Ac==nill to Rd
        End for
Step 2: check distinct data Dt
        For each attribute Dti in the data set
                While (mismatch attribute (Ac) == Rd)
                 Remove record set from rd
            Do
        End for
 Step 3: check numeric and non-numeric validated attributes fields
            If Rd is a numeric attribute
                        Then hold discretize or eliminate the attribute;
                            If Rd is a non-numeric attribute Then
                                Hold Values ←rd
            Else
                Remove the non-matched noise value
           End if
      End if
  Step 4: keep raw data originate all fill case record fields
  Step 5: create a cloud environment CE→ req/res
            If (req→valid)
             {
             Proceed CE←get access else till reject
             }end if
Step 6: validation checks for ordered records to authenticate CE
```

The above algorithm sanitizes to cleaning the noise in raw data (Rs) which it originates data without outliers form of distinct values and set up the cloud environment(CE). The preprocessing arises the raw data with a conventional field of each record as attributes empty case as Null field.

[Noordeen, 6(4): April 2019] ISSN 2348 – 8034
DOI- 10.5281/zenodo.2639756 Impact Factor- 5.070

3.2 service based exponential session time security.

In this stage, the service level is validated through the user request based on time by first establishing a shared data be encrypted at the time of evaluation. Same as the session integrates time authentication to encrypt the data with valid period time. The session expired the encryption states be varied due to requesting time. The data is on time verification to use for the intercommunication and not for encryption or decryption. Further, it's for allowing the data to the cryptographic policy. This session posses with two parties confirm that the transfer of the transfer process should not be known to each other before the evolutionary period of time has evolved to create a shared secret on the Internet. Keys interchanges between the owners and users they both end up with the same session key as a secret. Then each can easily calculate a third session key that cannot be obtained by the attacker who knows the two exchanging values. This key is encoded with subsequent contacts using a symmetric key.

Algorithm: Exponential session time security

Input: User Request Ur.
Output: on time session data security
Start
Step 1: Read user request Ur.
Step 2 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
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.
Else
Deny Access.
End
Stop.

The above-discussed procedure allows the comprehensive audit to operate or verifies user's trust to deny user request. The Service Access Key features generate a service level two statedoutsourced key on the state to decode the service data. In the centralized security service has the Privacy-Key, where all known service level public key is only provided commonly to user's ownership of the data first. But the quality of the service is based on the owner's request for data access selection.

3.3 Service Level Verifiable Attribute-Based Encryption on time

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 the 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.

[Noordeen, 6(4): April 2019] ISSN 2348 – 8034
DOI- 10.5281/zenodo.2639756 Impact Factor- 5.070

Algorithm: 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 BUser A 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

The SLVAE Enforcement Plan over time security solves the key leak problem of state encryption and some security properties with the session's efficient extension coding, semantics protection against selection-blank attacks. Session time encryption scheme. This program is a character based encryption. This means that the sender k ∈ Z * n and calculates the ciphertext C = (A, B) to hide a message to the server-wide main audit system with general parameters (n, e). K= ke (mod n) and B = m × (k + 1) e (mod n) ciphertext receiver first computation k = Ad (modn), then m = B / (k + 1) e (mod n). This process is shown to be semantic safe (due to the difference of k e and (k + 1) and mod n). This cloud service provider has been encrypted, and a cloud is encrypted by the user or the consumer. Once the data is publicly encrypted, it can only be done with the corresponding private key encryption. Session time uses the modular extension in encryption

3.4 Outsourced Verifiable key verification

A third-party audit (TPA) process can verify data based on time session verification. When receiving a request from the client to verify tons of data, it sends an audit message to the service provider requesting a set of data sets. The audit message contains the status of the modules requested. Service provider sets a linear combination of blocks and applies to a mask. Serving as a service provider authenticator and tons of masked modules. Finally comparing mask modules from metadata from customer service provider and client.

3.5 SLVAE Reverse decryption

The session time period verifies the SLVAE on time security based on the session request time key verification. The decrypting text is the process of tuning the original text (data) to the tie interval due to session time authentication.

Cloud client service provider initially requested cloud user data. The Cloud Service Provider is the Verity user's authenticity and provides the encrypted data by end-time session security. Time decrypts data by computing, m = cd (mod n), then checks with SLVAE security user's key authentication. The data is obtained from the original data source by changing the main user padding program.

To decrypt the original content from the ciphertext, c2 remain the key verification as follows
Step1 Verify the private key dA to process c→dA=K mod nA refers the ciphered content
Verify the session time resemblance key K→T(dA)
Step 2 based on the unique key integer verification Euclidean distance is estimated
Key point s →1<s<nA points $s * k \equiv 1 \pmod{nA}$.
Step 3 verfiy the message decrypted point c2 s = (meA k) s = (meA)k
Verified authentications = meA mod nA.
Step 4 decrypt message m in servce key private reference dA→ m:(mesA) dA = m mod nA.
Decryption process remains the unique key separate from the public key for decryption to attain the security. The two stated key h: $Zn \times Zn \rightarrow \{0, 1\}$ be create the hash function. The encrypted text verifies the TPA principles of the message (m). The referred term key in exponential ale is e→m of pointing key messages in message A→ke, message B→m*(k+1)*e. The service key description H = h(m, k).after the verified service level authentication the receiver retains the key to decrypt the original message.

IV. RESULT AND DISCUSSION

The resultant provides the execution of security SLVAE standard implementation by testing parameters using performance analysis in encryption, decryption and auditing state. The projected crypto policy-based data security using trust key verification in service access time in public auditing cloud security environment. The verification begins the auditing source of owner data logs with outsourced encryption and decryption suing station endpoint with valid time period interval to request the data. The collection of different content file size executed at in different level time taken to execute the process of encryption-decryption duration and integrate with auditing point. The implementation was carried out through visual studio framework 4.0 with SQL server authentication. The resultant given below shows the performance of proposed security proves the higher efficiency**.** The proposed SLABE, MARK-SLE,SLSBE implementation are based service level attribute encryption algorithm with outsourcing data encryption verifiable security be tested and evaluated for its efficiency. This security framework was performed using Microsoft visual framework 4.5 using c#.net cloud simulator with backend SQL server for log maintenance, and its security is increased based on overall performance.

Table 1: details of simulation parameters

Processed Parameter	**Value processed**
Service levels	5
Type of data	Data files
Number of users	3000
Service provider	CSP

The above Table 1, defines the value and parameters to process the service level security analysis. The public auditing efficiency assessed by utilizing the keygen policy of total key generated to verify correct access by submitting to auditing by or not a third-party auditor.

ISSN 2348 – 8034
Impact Factor- 5.070

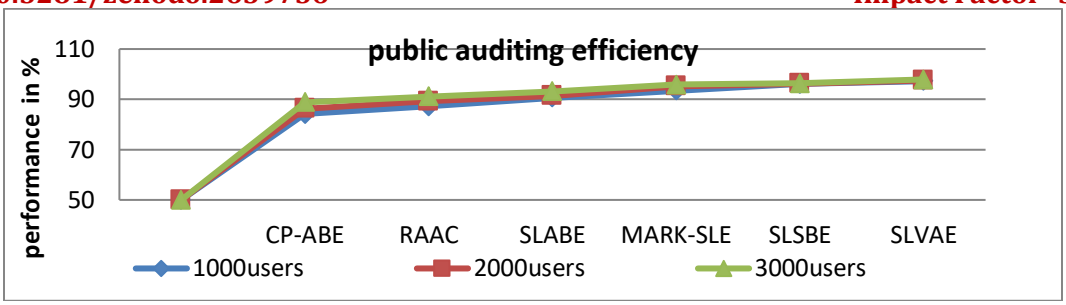

Figure 4: Comparison of public auditing efficiency

The above Figure 4, defines the performance of verification authenticity produced different methods using public auditing. The new implementation produced higher verification in third-party auditing services as well performance compare to other conventional methods

Table 2: Comparison of public auditing efficiency

Methods/users	Comparison of public auditing efficiency in%					
	CP-ABE	RAAC	SLABE	MARK-SLE	SLSBE	SLVAE
1000 users	87.2	90.6	93.4	96.1	96.8	97.2
2000 users	89.2	91.4	95.2	96.2	97.2	97.5
3000 users	91.1	93.2	95.8	96.4	97.5	97.9

The above table 2 defines the key authentication verification of public auditing proficiency with different methods the proposed system 97.2 % efficient than other compared methods. The security evaluation is overall performance of secured verification by the right key of access given authenticator do by encryption and decryption to deliver the secured service.

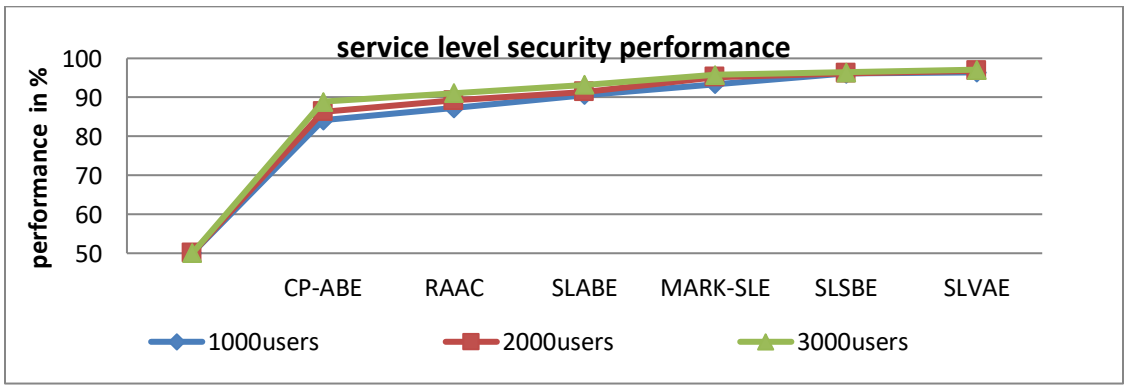

Figure 5 Comparison of service level security performance

The above figure 5 defines cloud the service level security for encrypting and decrypting process of security performance. The proposed configures service measure in each verification to improve the security compared to the other conventional methods.

ISSN 2348 – 8034
Impact Factor- 5.070

Table 3 Comparison of service level security performance

Methods/users	Comparison of service level security performance (%)					
	CP-ABE	RAAC	SLABE	MARK-SLE	SLSBE	SLVAE
1000 users	87.4	90.3	93.4	95.6	96.2	96.4
2000 users	91.7	92.1	94.2	95.7	96.4	96.8
3000 users	92.4	92.8	94.8	96.2	96.7	97.1

The cloud service level security performance is shown in above table 3 with different methods the proposed system 96.4 % efficient than other compared methods. The time complexity is evaluated by a total number of request to verify by the logs to access the data with the time of preference.

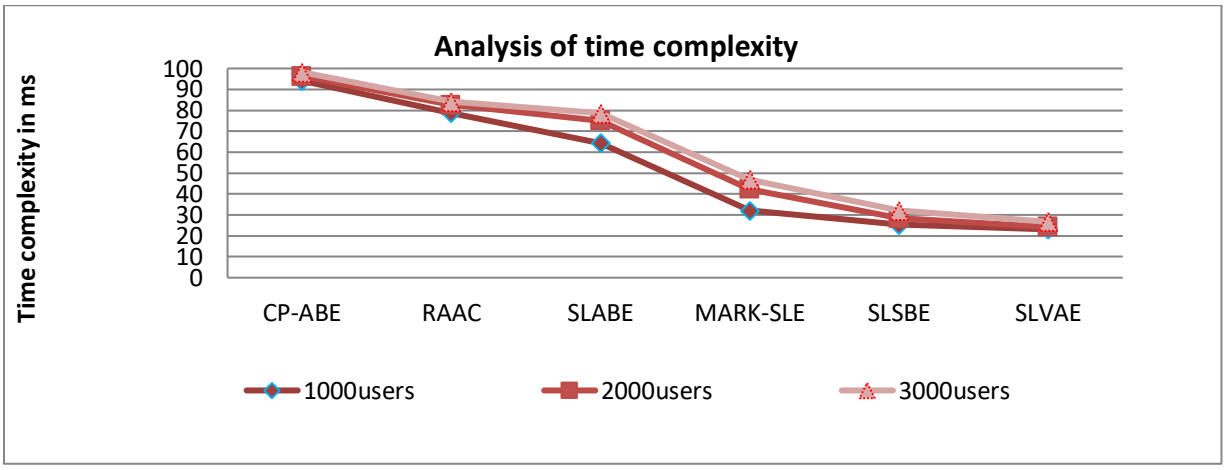

Figure 6: Comparison of time complexity

Figure 6 defines the corresponding effect on the execution strategy complexity time produced in different conventional methods, and it is clear that the proposed method produced less complicated time than other methods.

Table 4: Comparison of time complexity

Methods/users	Comparison of time complexity in Mille-seconds (ms)					
	CP-ABE	RAAC	SLABE	MARK-SLE	SLSBE	SLVAE
1000 users	94.1	78.7	64.3	31.2	25.3	23.1
2000 users	96.3	82.6	75.1	42.3	28.4	24.2
3000 users	98.2	84.1	78.5	46.9	32.1	26.7

Table 4 defines the comparison of Different Methods in the Table above Comparison of the Critical Time in Milli-Seconds. The proposed system 23.1 (ms) is more efficient than dynamic display compared to other.

V. CONCLUSION

The conclusion proves the Service Level Verifiable Multi Attribute-Based Encryption (SLVMAE) intents the best security performance using the session time key verification for securing the data in cloud data. The proposed

system achieves high performance compared to the other system. The method classifies the services with a time of authentication and data as auditable service as higher end security with the regular interval. 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. The data encryption and public auditing are enforced in service level which increases the performance of session time public auditing as well 96.4 % well time complexity 23.1 milliseconds. The proposed method improves the performance in public verification, throughput and reduces the time complexity as well.

REFERENCES

1. *Henning, R. Security service level agreements: quantifiable security for the enterprise? In Proceedings of the 1999 workshop on New security paradigms, NSPW '99 pages 54–60, New York, NY, USA. ACM,2000.*
2. *R. R. Righi, F.R. Pelissari and C.B. Westphall, "Sec-SLA: Specification and Validation of Metrics to Security Service Level Agreements," in IV Workshop on Computer System Security, pp. 199–210. SBC Press, Porto Alegre, 2004.*
3. *F. Guo, Y. Mu, and Z. Chen, "Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key," in Proceedings of Pairing-Based Cryptography (Pairing '07), ser. LNCS, vol. 4575. Springer, pp. 392–406, 2007.*
4. *Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09, volume 5789 of LNCS. Springer-Verlag, pp. 355–370,Sep. 2009,*
5. *Z. Zhang, D. Wong, J. Xu, D. Feng, Certificate less public-key signature: Security model and Efficient construction, in Applied Cryptography and Network Security, Vol. 3989 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, pp. 293–308, 2006.*
6. *Q. Wang, C. Wang, K. Ren, W. Lou, J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel And Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.*
7. *Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 1, pp. 647-651. IEEE, 2012*
8. *Gurudatt Kulkarni, Ramesh Sutar and Jayant Gambhir, "Cloud Computing-Storage as Service," International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 1, pp.945-950, 2012*
9. *Y. Zhu, G. Ahn, H. Hu, S. Yau, H. An, S. Chen, "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 227-238, 2013.*
10. *Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, "Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Transactions on Communications, vol. E98-B, no. 1, pp.190-200, 2015.*
11. *L. Ferrara, M. Greeny, S. Hohenberger, and M. Pedersen, "Practical short signature batch verification," in Proceedings of CT-RSA, volume 5473 of LNCS. Springer-Verlag, pp. 309– 324, 2009,*
12. *S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE - Simple Privacy-Preserving Identity-Management for Cloud Environment," in Applied Cryptography and Network Security - ACNS 2012, ser. LNCS, vol. 7341. Springer, pp. 526–543, 2012.*
13. *M. Rak, N. Suri, J. Luna, D. Petcu, V. Casola, and U. Villano, "Security as a service using an SLA-based approach via SPECS," in Proc. of CloudCom, 2013 IEEE 5th Int. Conf. on, vol. 2, pp. 1–6,Dec 2013.*
14. *J. Lai, R H Deng, C. Guan, and J. Weng. 'Attribute-Based Encryption with Verifiable Outsourced Decryption.' IEEE Trans. Inf. Forens. Security, vol 8, pp 1343-1354, 2013*
15. *J. Sidhu and S. Singh, "Improved topsis method based trust evaluation framework for determining the trustworthiness of cloud service providers," Journal of Grid Computing, pp. 1– 25, 2016.*
16. *Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H.Deng, "Key-Aggregate Cryptosystems for Data Sharing in Cloud Sharing," IEEE Transactions.2016.*
17. *Huijun Zhu; Licheng Wang; Haseeb Ahmad; Xinxin Niu," Key-Policy Attribute-Based Encryption With Equality Test in Cloud Computing," IEEE Access, Vol 5, pp 20428 – 20439,2017.*

18. *S. Ohata, Y. Kawai, T. Matsuda, G. Hanaoka, K. Matsuura, "Reencryption verifiability: how to detect malicious activities of a proxy in proxy re-encryption," CT-RSA 2015, LNCS 9048, pp. 410-428, 2015.*
19. *Prakash G L, DR. M. Prateek and Dr. I. Singh, 'Data encryption and decryption algorithms using key rotations for data security in the cloud system.' IEEE, 2014.*
20. *Feng Wang; Li Xu; Wei Gao,"Comments on "SCLPV: Secure Certificateless Public Verification for Cloud-Based Cyber-Physical-Social Systems Against Malicious Auditors," IEEE Transactions on Computational Social Systems, vol 5, pp 854 – 857,2018.*