AN IMPROVING CLOUD DATA SECURITY STANDARD USING PRIME PADDING ATTRIBUTE BASED ENCRYPTION WITH SUPPORTIVE SERVICE LEVEL DYNAMIC AUDITING IN CLOUD ENVIRONMENT

D.Prabavathi[1] and Dr. M. Prabakaran[2]

[1]Research Scholar of Bharathidasan University, Assistant Professor of Computer Science, Srinivasan College of Arts and Science, Perambalur, Tamil Nadu, India.

[2]Research Supervisor, Asst. Professor, Department of Computer Science, Government Arts College, Ariyalur, Tamil Nadu, India.

Abstract

Day by day Internet communication, data security, due to the problem of leakage of development data. So the cloud environment is needed to secure centralized storage data, privacy, and better protection levels for key management. The security key is the key to the most critical factor in protecting public key cryptographic data encryption. To overcome the problem, we propose a cloud data security standard using Prime padding attribute based encryption with supportive service level dynamic auditing in cloud environment. (P^2ABE-SDA).The proposed system integrates the prime factor random encryption (PFRE) to improve the dataset security. Data supplied by the chipper Volume Generic Key Generation algorithm with an additional padding program to improve service-level audit. Third-party prime dump integrates the main stored data embedded in single-saving. This system increases the dynamic factor of the publicly centralized cloud encryption protocol security system.

Key words: cryptography, key management, auditing, security, padding scheme, cloud storage.

1. Introduction

Developing internet security in centralized environment is widely developed and share the sources of data between the user be probable to communicate the information. The data store be directly accessed and stored in large data centers from server computers to a large distance such as databases. Creates customer data on a remote server and stored. The customer can then access data and access data using internet technology to save it. This technology provides web service on a reliable cloud computing platform, but it also various attacks on accessing data and performance issues be occurred without verifying the data to provide. Auditing and data leakage is big problem in security saving issues. Data stored in a remote server data integrity is not incredible. The service provider doesn’t have problem security against the attribute based cryptography to cover customer marginal security. As a result, server access rarely removes the customer. Knowledge of the need for customer needs to be followed by observing the data integrity of data retrieval.

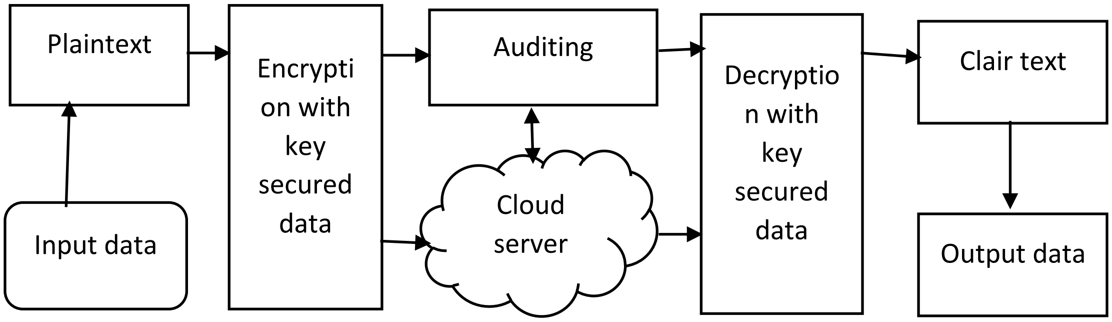
Plaintext
Input data
Encryption with key secured data
Auditing
Cloud server
Decryption with key secured data
Clair text
Output data

Figure 1 Public key cryptographic security process

Cryptography is a combination of data mathematical handling (cryptosystem text) for both text (key). Convert text using the text encryption key encryption algorithm used. And the use of the decryption algorithm used to change the cursory text text on the key chipper text. Some important algorithms are required before creating the encryption and removal algorithm. During the encryption, there are three basic process-key generation, encryption and decryption process.

The problem is that many proposed systems are solved by data integrity. Security concerns begins from the owner providence and auditing state of access. TPA auditing program affords more effectiveness when any public examination, allowing only the savings cloud server to handle customer-based data while keeping any personal information. Employee General, The Client's Third Party auditor (TPA) generates a public key initialization to afford the data security. Done is stored on remote file server Customer informs about the stored file monitoring and protection. RSASS is a data censor system stored on a remote server. This instantiation is based on frequent testing and synergies often tested for challenging server clients with a method based on the RSA Signature Algorithm. Invalid server detection provides maximum probability when the RSASS identification method exists. Using this method is the place where the server is in use and can be used to change the volume of the blocks so that the calculation time is reduced.

There are a lot of algorithms available in the encryption area. This is followed by AES back DES, 3DES and balloon fish algorithms. So, in my work, my algorithm is slightly compared to these protocols. XOR is made of these different kinds of algorithms such as bitwise, substitution, replacement and so on

2. Literature survey

The cryptography system in traditional certification verification includes the user's public key and its owner's identity to access the key randomization length. Important therefore some trustworthy authority must have a certificate based on the user's identity [1]. The digital identity must be verified by the authority signal by the auditor.

A signer cannot expect this to be a public key signature and that he does not know the relevant access key verified by outsourcing auditing[2]. The standard argument against such an approach is the functional interference of the cryptographic system. However, we both show that patients are able to create part of their access to partial access with others and show that they are able to make more searches for their recordings.

The cloud is calculated computationally computing devices [3] is a formidable job for users. Its integrity It savings management, global data access, can also use cloud storage for users who are not worried about the need to verify their burden is published in authentication policy. Problem raised on different signs verification in fact that corporate hardware computing is more efficient, therefore hardware, [4], software and employee maintenances costs hardware.

There are many authoritative cloud storage systems where many of the authorities were in collaboration and capable of providing free access to each authority [5]. In particular, we propose basic strategies, many changeable Communist Abbey plans and apply it to the data access control program design. Our characteristic security and backward security both have been canceled in a safe way.

Introduction to tone is that the customer's involvement in the cloud-saving data can be the size of the economies for cloud computing, which is actually perfect. [6] The most significant forms of block transformation, insertion and deletion data, such as surgery, dynamical data via support, and not only an archive or backup data in cloud computing services, but also a significant step towards practicality.

Traditional safety issues are still in the cloud computing environment. Corporate definitions are also issued by cloud but [7], which are no longer suitable for traditional safety guidelines and data in cloud applications. Cryptographic support programs proposed on encrypted data encoding questions. They are all but important recursive data requiring expensive re-encryption, accessed by a single user or a key depending on a set of secret keys that many users share among the keys. Instead of specifying what data the network would be used to do for a backup, you can specify what should be done for the backup of the larger ribbon library and shop for the backup (shop) tapes [9], organized by a network administrator.

Real-time efficiency monitoring service [10] and the use of this or the untrusted theoretical and outsourced savings to verify the integrity of the service to determine how they are determined by changing adaptation to adjust to the short-term variation by expanding and packaging the resources. Our audit service techniques [11, 12] are structured based on updates supporting fragmentation, random sample, index-hash table, outsourced data and proven timely disorder. To combat information leaks, we have zero-knowledge techniques that hide the integrity test process.

The main search technique in traditional and efficient simplicity is to use subtle data to preserve data that is useless [13] Outsourcing, the data owner must be hidden before. So the accuracy and efficiency of the two objectives [14], how to design an efficient, encryption of cloud data is a searchable encryption scheme on a very challenging task.

In some cases, some proxy [15] is available to test work for remote data. However, some state information on proxy cloud storage servers [16] is notable because these PDP programs are not safe. Simple pre-plans, a semi-reliable party modeled as a proxy, and the recryption process is considered to be done significantly honestly. We believe that trusted representatives [17] need to do this relatively high level, before it, e.g. Some applications may be unlikely cloud-based file transfer systems.

Constant volume of ownership New texts generating public key cryptographic methods Decrypting gyratory texts are available to any set of efficient group [18]. Attribute-based encryption (Abe) to protect users' identity. Abe is widely used in most of the [19] locations especially in cloud computing. In this analysis, the equality test connects to the public key encryption key-policy. It is important for users to manage data, [20] a simple, cost effective, and flexible way of outsourcing cloud server data, whereas users have their data on their outsourcing data cloud servers Losing control.

There are a lot of problems when all the studies on mechanisms are found. Like...

1) The most complex system of instruction increases the execution time. So simple do-it-to-do structure should be fast algorithm.

2) Compared with longer lengths to provide longer protection as a length key, the speed of the execution will increase.

3) Depending on the math and / or logo activities on text, key and rotation text used in any algorithm for overall performance of the selection. My method, all these steps consider issues that improve encryption performance.

3. Implementation of proposed system

Cloud Security and Service Provider Cloud is the most important document among these which are still subject to further permission to manage the data that provides the level of key data in the place where only the work is allowed. Clients need cloud security on the effects of performance system and the cloud providers have yet to find a number of methods to connect data to maintain their form data. In this proposed system we implement a Cloud data security standard using Prime padding attribute based encryption with supportive service level dynamic auditing in cloud environment. This Maintaining the content of own content and then increasing the level of the analyzes and clouds to document their information efficiency on encryption.

Because of the vast area of communication and use of a wide variety of purpose and use of the client of the cloud, the most important security problem is because the point is to hack others to the cloud data interest. Therefore, we focus mainly on the process of encryption and removal of security information using the Cloud Computing port. It can be used here but still depends on a number of correct algorithms, which can be somewhat safer for the entire data to focus on secuirty concerns.

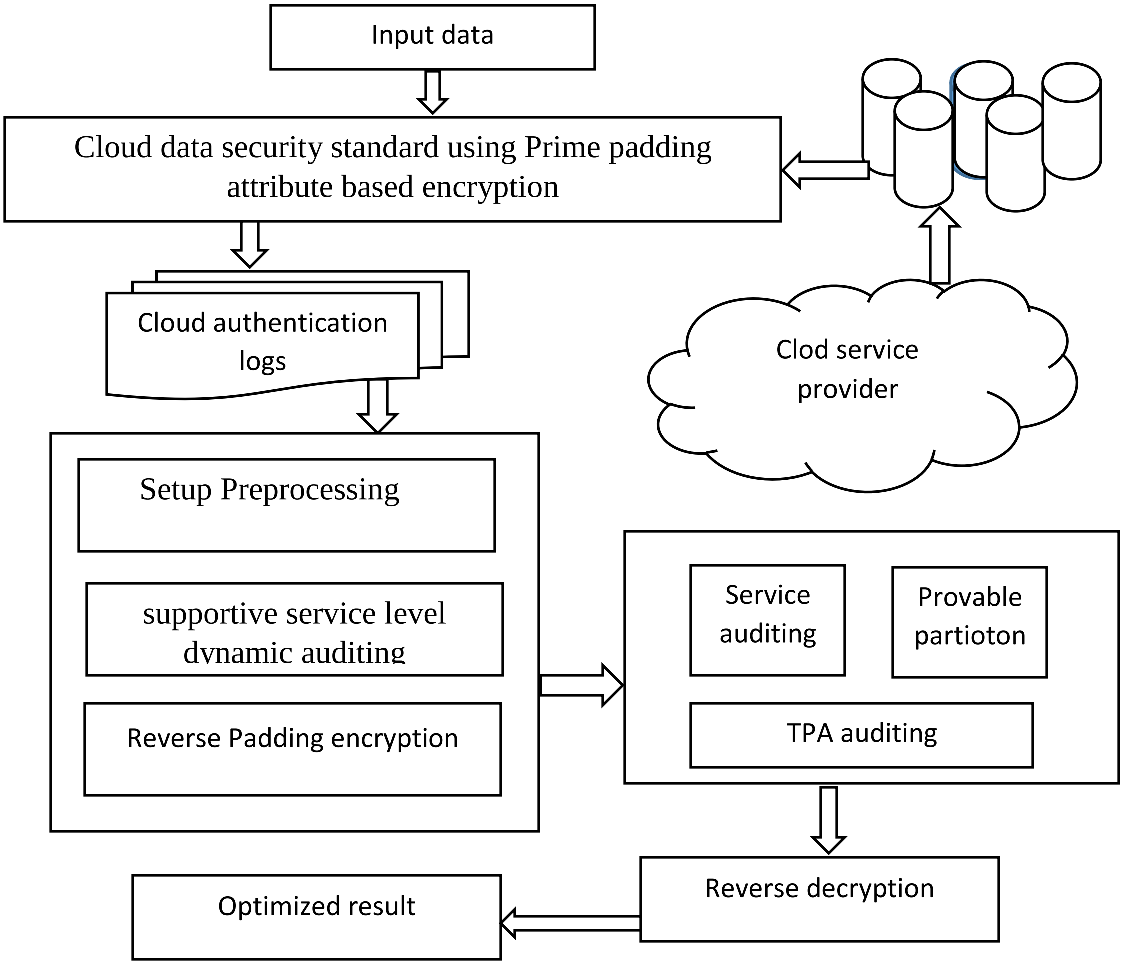
Input data
Cloud data security standard using Prime padding attribute based encryption
Cloud authentication logs
Clod service provider
Setup Preprocessing
supportive service level dynamic auditing
Reverse Padding encryption
Service auditing
Provable partioton
TPA auditing
Reverse decryption
Optimized result

Figure 2 Architecture diagram for proposed system

RSA Security standards (RSASS), a storage system based on the RSA signature algorithm, is continuously monitored for the security of its stored data. It is proven to be based on data modeling

Use the provable partition method to verify the data after the security to verify the client request to monitor the action to access the data. Right verification defense the challenges of cloud security to splits the key standards , data standards etc. the splatted blocks are subdivided into the remote file server and have the proof of its value for the selected Subcommittee volumes. The customer checks verifications it is retrieved request responses and makes sure the remote cloud packing file is correct to the server. The RSASS has two phases, ie system structure and integrity.

Field Safety: (1) Due to the dynamic measurement, service essence cloud computing models have the ability to use data cloud platform applications and any standard infrastructure and security boundaries due to location transparency specializations. If a security breach involves, it is difficult to isolate a particular resource that has a physical threat or is left out.

(2) cloud computing service distributes cloud services based on resources that may be owned by many providers, according to distribution models. If there is an interest paradox, it is difficult to sort out a united defense operation

(3) multi-tenant cloud and virtualized by the openness in sharing resources, such as access to user data and other unauthorized users.

(4) Cloud Platform To meet massive information storage and provide fast access to a cloud, cloud security will also meet the need to use massive information processing operations.

Key features of proposed system

1. It is a special trusted domain-based and boxes must manage a trusted agent in each domain. A Cloud-based service provider resources are a trust management. 2. It distinguishes between two different roles in the cloud: Designer designs for more customer deliveries and different credibility for the customer. 3. Relieve Reliance Establishing Reliance on Reliability and Conducts Trust of One Kind of Service. 4. The decision factor and refresh take time factor and factor transaction into account.

3.1 Setup Preprocessing

This stage preprocess planning security tasks in cloud systems, select how to effectively exploit resources to share other than duplicates and resources to utilize fully. At the same time, communication plays a major role in delaying cloud planning delay, which leads to great waiting between security dispense but can cause idle time interval between processing units. In this thesis, a removal setup system uses efficient preprocess cloud resources. Planning program, directed by outlier Map Previous coating time based planning is called a multi-cloud duplicate systems algorithm and a new protocol is included in the secuirty of reconstructing tasks in the list. The copper time attempts to replicate photo insert the appropriate immediate security from removal of filled non filled verfrication of the current terminal of the processor selected in order to reduce its waiting time.

Algorithm

```
Step 1: Input raw data Rd {rd1,rd2,…rdn}
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
    Step5: validation checks for ordered records
```

The preprocessing crude data for each record field arises with empty attributes as a regular field empty case. The above method of cleaning sanitizes the noise of raw data (Rs) values without which it originates in the form of distinct data acquisition.

3.2 Supportive service level dynamic auditing

This condition is distributed in favor of the service provider distributed by the supervisory power servers. This company is considered semi-reliable. Private audit is system configuration. The model consists of two companies and the owner of the cloud service provider information. This framework allows the information owner to only process the information to verify the information structure established by the repository server relating to the distribution and operation of the company. TPA wants a challenge to verify that it is at any time to verify the distant server information. Server has been certified by a source that retained that information. The correct evidence confirms that the encryption keys are used by the information matched by the tons and is generated by the right statement.

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

```
                    Perform data management.
            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.

Since the outsource information is naturally changing, it is necessary to set up a dynamic review of the Outsourcing Information Conference on Operations. Intuitive authenticators are used to achieve a standard transmission overhead in a general verification mode. In the previous procedures, the valuation will be recognized as the creditor's value as the same creditor and used to evaluate the distributed server through the process of evaluating the owner's permission to block the distributed server. The three equations are not replaced by three K, KP and KQ equations: ED = K 0 (n) +1 = K (p - 1) (Q - 1) +1 equation (5.1.1) = k (n - p (q 1) + 1 (5.1.5) + 1 (5.1.5) edp = kpho (p) + 1 = kp (p - 1) + 1 (5.1.6) edq = kqφ (q) + 1 = kq (q - 1) + 1. However, the insertions are limited to using the token value of the chunk that they may develop complex. Information needs to be chunky tags so that the real cloud is the best in all of the subsequent scenarios where the information itself will be refreshed. As a result, the totally variable tag token function has to do with the valuation process to prevent them from fulfilling verification state.

3.3 secured PDP data in Prime factor encryption

As an imaginary one can do, there is a need for encryption sources for longer forecasts for stronger security. Performance and safety level and safety levels measure the relationship between the ABE offers and the inspection to determine what level of security is. The coordinate-based encryption ABE is built on top of its security paired oriented cryptographic algorithmic base strength

1. Two different Big Random Numbers are selected by B & K.

2. Compute, $n = k \times p$.

3. Predict: Phi (N) = (PQ-1) (Q-1).

4. Compute the prediction 1 <e

The user B is encrypting an informative m, with which one decrypts the user. User needs to do the following to B:

- Receive a true public key (NA, EA).
- [0, NA - 1] to specify a full m message at intervals.
- compute the such as GCD (K, NA)) →process of random value g 1 <Q <NA,.
- repeated progress C1 = k EA mod n compute value.
- process c2 → Foreign k mode.
- Send User A to encrypt text message (C1, C2).

The main characteristics of a pivotal introduction of prime padding include encryption embedding bits, protection against the defenses of semantics and some protection of semantics. The program was distributed 6 times faster than the main pudding in David encryption. This program is an RSA-encoding version of the main padding. That is, in order to encrypt a message m for the RSA system with public parameters (n, e), the sender chooses k ∈ Z ∗ n and computes the ciphertext C = (A, B), This project is not semantically preserved. The big integer factor. The hardest attack is to send a lengthy enough public key encryption key length to the origin and structure of the well-arranged group of distributed net users, as the new factor and methods of improvement in the performance of the methods developed by the methods. where, A = k e (mod n) and B = m × (k + 1) e (mod n). Subscriber receiving the first computation by pressing Q = advertising (modn), and m = / (k + 1) e (mod n), retrieves. (Q + and (k + 1) emod n, due to distinguishability)

3.4 Reverse decryption auditing on TPA

The third party audit (TPA) can verify the main padding data. When receiving a request from the client to verify tons of data, it sends an audit message to the service provider asking for a set of data sets for verifying auditing policy. The audit message contains 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 wires. Finally comparing mask modules from metadata from customer service provider and client.

Following are the reverse decrypt to verify the private key,

The request c2 remains plaintext to user A

- The dA be the private key C
- Compute the [process dA→k mod nA.
- To represent the unique integerts based on eculidian estimation integrt s to compute $1 < s < nA$, such that $s * k \equiv 1 \pmod{nA}$
- Compute c2 s = (meA k) s = (meA) k s = meA mod nA.
- Compute (meA) process→ dA = m mod nA. access level from provate key to recover m to use

This prime padding reverse decryption is a strengthened version of encryption in order to secure protection. Zinc × zinc → {0, 1} L is a hash function: l let a safety parameter and hours. A = Q E, B = × (k + 1) e m, and H = h (m, k): A three m (A, B, H) of a database m. Here k is a random value. If the cipher is to be decoded, the receiver calculates: Q = ad (mod n), and m = b / (k + 1) e (mod n), then equality H tests? = H (m, k). If equality is satisfied, the information m is agreed; Otherwise, Cypertext rejected. This program does not seem to be aware of Cybertex, as it is a news probability, the ACCA is not safe against.

4. Result and discussion.

The resultant provides the execution of security 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 public auditing cloud security environment. The verification begins the auditing source of owner data logs with outsourced encryption and decryption suing station endpoint. 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

Table 1: Details of processed parameters

Parameter	**Value processed**
Service provider	Cloud service provider
Data processed	File Type, Clair text
File size	25 mb,50mb,75mb nearer
Number of users	1500

The above table 1 shows the parameters and the values taken to test the proposed system implementation. This contains a cloud service provider that is centralized to process the authentication with encrypted cloud data. The data that are proceeding in the form of Clair content in different file size to test the security.

The impact of security analysis

The security depends on the process of encryption with key possess the auditing strategy to take the overall execution.

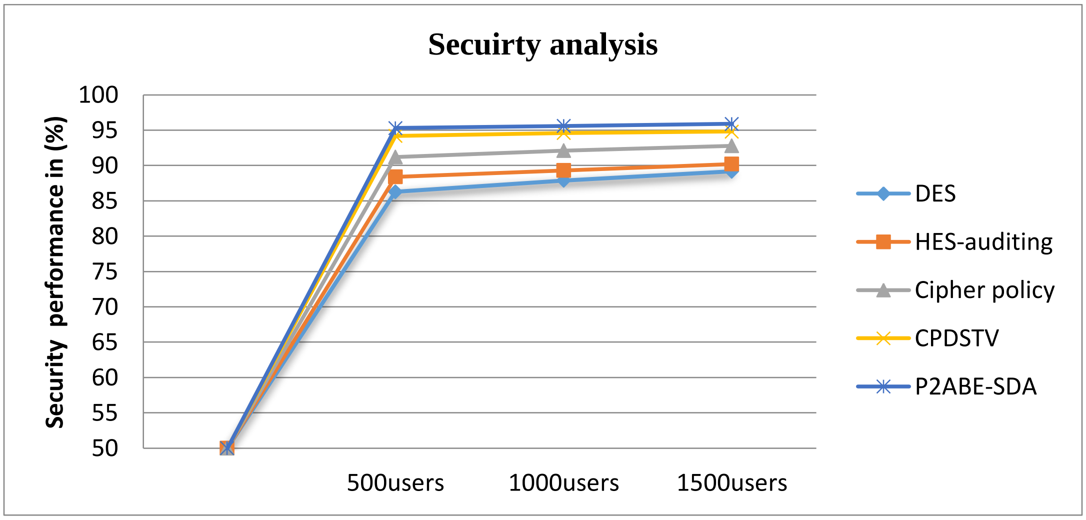

Figure 3: Comparison of security analysis

The above figure 3 shows the different methods produce the different level of user to do the security activity. The proposed system produce the higher impact security performance compared to the other dissimilar methods.

Table 2 Comparison of security analysis

	Comparison of security analysis				
Methods /users	DES	HES-auditing	Cipher policy	CPDSTV	P^2ABE-SDA
500users	86.3	88.4	91.2	94.2	95.3
1000users	87.9	89.3	92.1	94.6	95.6
1500users	89.2	90.2	92.8	94.8	95.9

The above table 2 shows a comparison of the Security analysis, and this can be tested with the total number of users that access the security with right authentication to access the data. The proposed system produces 95.9 % accuracy compared to the other methods. The proposed system proves the great performance of higher-end security with the improvement of standard crypto advanced efficient.

Impact of key auditing during encryption and decryption

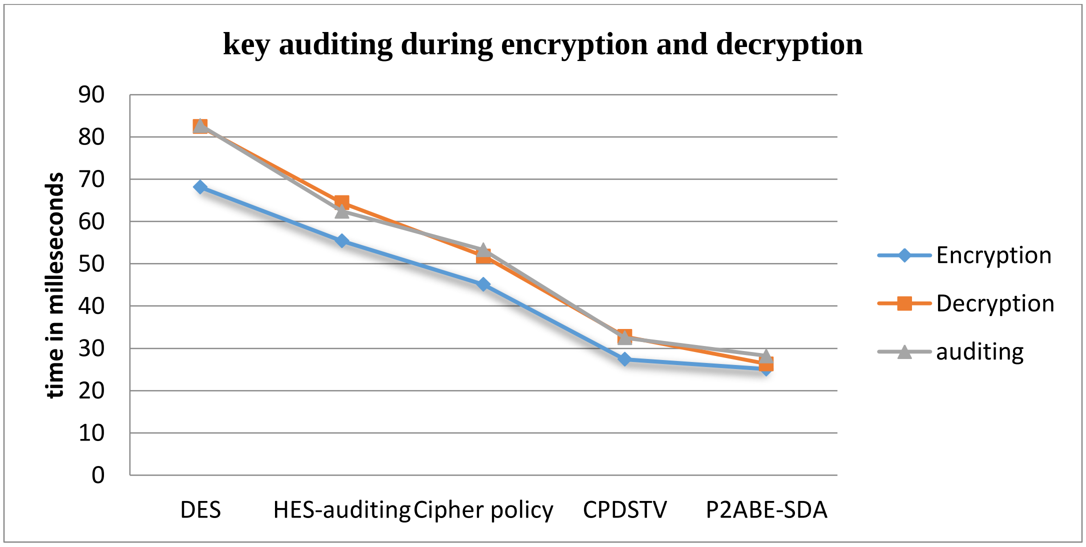

Figure 4: Comparison of key auditing execution

The key verification proves the security to provide right authentication for whom have the right key to request the data. Time is taken to encrypt the data with key generation based on the size of the data. Similarly, the decryption has time taken to verify reverse encryption with verified key logs.

Figure 4, shows the efficiency of execution state processed between encryption and decryption whether the key is auditing at the meantime 25.1 ms as well as DES cipher policy. This implementation had much-improved performance compared to previous methods.

Table 3 Comparison of key auditing performance

Methods/state	Comparison of key auditing execution during encryption and decryption				
	DES	HES-auditing	Cipher policy	CPDSTV	P^{2}ABE-SDA
Encryption	68.1	55.4	45.1	27.2	25.1
Decryption	82.4	64.2	51.8	32.3	26.3
Auditing	82.7	66.4	53.4	32.7	28.2

Impact of time complexity analysis

The overall time is taken to encrypt the data based on the size which depends on the process of execution. The time leads the fact with differential Clair content had the crypto policy security standard. The proposed system produces the lower time to process the data and improve the security which doesn't have time given to the intruders.

Time complexity (Ts)=$\frac{\text{Total number of blocks per bits} \times \text{two phase encryption}}{\text{time taken (s)}} - - - (1)$

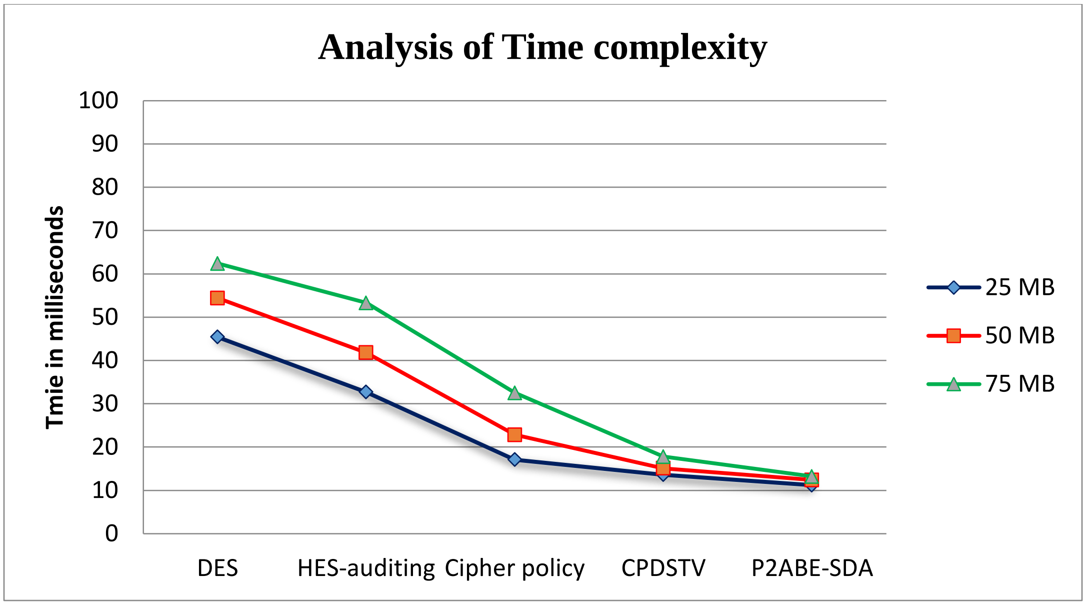

Figure 5: analysis of time complexity

The above Figure 5 shows the various file size to handle the encryption at mean time of evaluation by dissimilar methods, and proposed system P^2ABE-SDA provides the least time 13.2 ms as well as previous cipher policy. This implementation had much-improved performance compared to prior methods.

Table 4 Comparison of time complexity

Methods/different Clair text file size	Comparison of time complexity				
	DES	HES-auditing	Cipher policy	CPDSTV	P^2ABE-SDA
25 MB	45.4	32.7	17.1	13.6	11.2
50 MB	54.4	41.8	22.8	15.1	12.4
75 MB	62.4	53.3	32.5	17.8	13.2

The above table 4 shows the comparison time complexity which the proposed system produces higher improvement than other methods. The proposed system produce least time complexity of execution than other methods.

Impact of false occurrence

The false occurrence is states of verification at the service level of integrity during key failed state, or encryption and decryption state.

$$\text{Frequent occurrence state (FS)} = \frac{\text{Repeated block of the cipher}}{\text{Total number of cipher block occurrence}} ----(2)$$

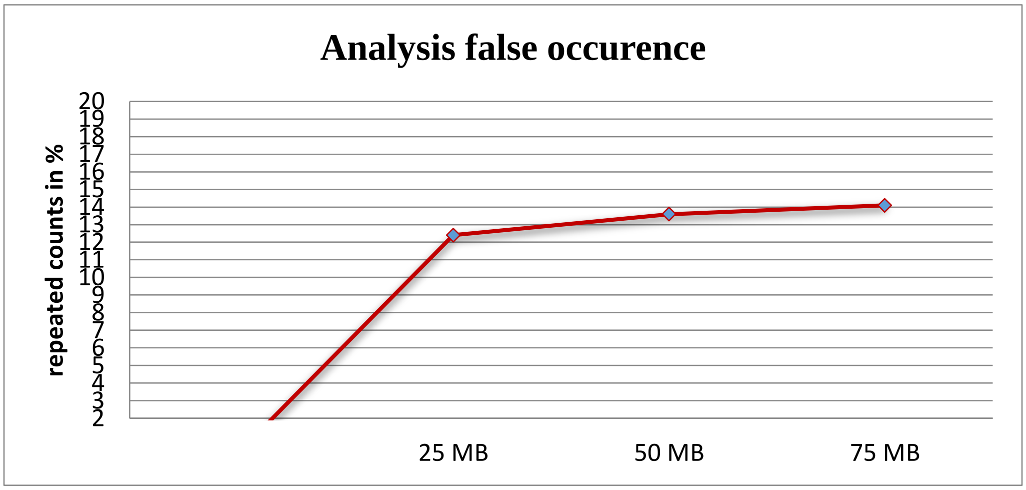

Figure 6: Comparison of false occurrence

The above Figure 6 shows the failed states to do the encryption whether data is encrypted during non-redundant evaluation with dissimilar methods. This shows evidently our implementation of proposed crypto method has produced active redundant false rate than previous methods.

Table 5 comparison of false occurrence

Methods/different Clair text file size	Comparison of false occurrence				
	DES	HES-auditing	Cipher policy	CPDSTV	P^2ABE-SDA
25 MB	12.4	10.4	8.3	5.6	5.2
50 MB	13.6	11.2	9.1	6.1	5.6
75 MB	14.1	12.6	10.7	7.4	6.2

The above table 5 reviews the impact of execution at false evaluation of lower complexity by different methods. The projected method proves the least failure state in 5.2 % best evaluation to do the process quickly similar than other methods.

5. Conclusion

Data secrecy cloud storage is a major problem. Privacy with encryption tools can be confirmed. In this thesis, we are going to introduce a system that supports cloud general storage of cryptosystems on a variety of classes that support a general key cryptosystem to suppress secret keys. Our proposed method needs to be improved by providing advanced dynamic auditing prime padding system. Our job is to control the number of control classes and the front number of text. This issue can be solved by the public key extension. The performance of attribute based prime padding produced higher accuracy 95.9 % well compared to the other system at in higher security with lower time complexity with the state of execution.

References

1. D. Boneh and M.K. Franklin, Identity-Based Encryption from the Weil Pairing,‖ Proc. Advances in Cryptology (CRYPTO ’01), vol. 2139, pp. 213-229, 2001.
2. 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, 2006, pp. 293–308.
3. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,‖ Proc. ACM Workshop Cloud Computing Security (CCSW ’09), pp. 103-114, 2009
4. C. Wang, Q. Wang, K. Ren, W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing”, INFOCOM 2010, pp. 1-9, 2010
5. H. Wang, Identity-based distributed provable data possession in multicloud storage, IEEE Transactions on Services Computing 8 (2) (2015) 328–340.
6. K. Yang, X. Jia, Expressive, eþcient, and revocable data access control for multi-authority cloud storage, Parallel and Distributed Systems, IEEE Transactions on 25 (7) (2014) 1735–1744.

7. 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.
8. 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
9. C. Dong, G. Russello, N. Dulay. “Shared and searchable encrypted data for untrusted servers”, Journal of Computer Security, pp. 367- 397, 2011
10. 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
11. Magoutis,”Managing Service Performance in Data Store Distributed Storage system”,2013 IEEE International Conference on Cloud Computing Technology and Science.2013.
12. 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.
13. J. Zhang, W. Tang, J. Mao, “Efficient public verification proof of retrievability scheme in cloud”, Cluster Computing, vol. 17, no. 4, pp. 1401-1411, 2014.
14. Prof. Vishwanath S. Mahalle, “Implementing RSA encryption algorithm to enhance the data security of cloud in cloud computing”, International journal of pure & applied research in engineering and technology, 2013, volume 1(8):220-227, ISSN-2319-507X IJPRET.2013
15. 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.
16. Y. Ren, J. Shen, J. Wang, J. Han, S. Lee, “Mutual verifiable provable data auditing in public cloud storage,” Journal of Internet Technology, vol. 16, no. 2, pp. 317-323, 2015.
17. 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.

18. 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.
19. 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.
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.