ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

Efficient Double Encryption in Cloud Computing

S.Durga, P.Alagusundaram

M.E. Computer Science and Engineering, Department of Computer Science and Engineering, Mahath Amma Institute of Engineering and Technology, N.M.Nagar, Ariyur, Sithannavasal Road, Pudukkottai, Tamilnadu, India

Assistant Professor, Department of Computer Science and Engineering, Mahath Amma Institute of Engineering and Technology, N.M.Nagar, Ariyur, Sithannavasal Road, Pudukkottai, Tamilnadu, India

ABSTRACT: The main objective of this system is to provide the highest safety measure to remote server users with Authenticated Key Exchange Scheme using MD5 logic. As well as by the appliance of Proxy Reencryption scheme using Identity Based Provable Re-Encryption technique. Cloud Computing, a global medium which allows users to preserve their data securely in remote place as well as easy to share the data around globe without any delay. In storage services with huge data, the storage servers may want to reduce the volume of stored data and to monitor the integrity of their data with a low cost. Data duplication is an important issue to be overcome with the cloud services, which reduces the storage and the cost wastage. So, that a new scheme is introduced to avoid the duplication storage over cloud environment with proper security called Deduplication Elimination Algorithm. As well as, Identity Based Provable Re-Encryption is introduced to reencrypt the encrypted data to prolong the data security in high manner. Key Generation Algorithm is used to generate the random keys while processing the data and pushed into server.

KEYWORDS: Cloud Computing, Data-Deduplication, Cryptography, Data Security, Information Security, Public Audit, Secure Deduplication.

I. INTRODUCTION

In cloud storage services, clients outsource data to a remote storage and access the data whenever they need the data. Recently, owing to its convenience, cloud storage services have become widespread, and there is an increase in the use of cloud storage services. Well-known cloud services such as Dropbox and iCloud are used by individuals and businesses for various applications. A notable change in information-based services that has happened recently is the volume of data used in such services due to the dramatic evolution of network techniques. For example, in 5G networks, gigabits of data can be transmitted per second, which means that the size of data that is dealt by cloud storage services will increase due to the performance of the new networking technique. In this viewpoint, we can characterize the volume of data as a main feature of cloud storage services. Many service providers have already prepared high resolution contents for their service to utilize faster networks. For secure cloud services in the new era, it is important to prepare suitable security tools to support this change. Larger volumes of data require higher cost for managing the various aspects of data, since the size of data influences the cost for cloud storage services. The scale of storage should be increased according to the quantity of data to be reduce the volume of data, since they can increase their profit by reducing the cost for maintaining storage. On the other hand, clients are mainly interested in the integrity of their data stored in the storage maintained by service providers. To verify the integrity of stored files, clients need to perform

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

costly operations, whose complexity increases in proportion to the size of data. In this viewpoint, clients may want to verify the integrity with a low cost regardless of the size of data. Owing to the demands of storage servers and clients, many researches on this topic are available in the literature.

In 1998, Blaze, Bleumer and Strauss proposed the concept of proxy re-encryption (PRE), where a semi-trusted proxy can transform a ciphertext for Alice into another ciphertext that Bob can decrypt. However, the proxy can learn nothing about the corresponding plaintext. According to the direction of transformation, PRE schemes can be classified into two types, namely, bi-directional or uni-directional. A PRE scheme is called bidirectional if the proxy can use the reencryption key to divert ciphertexts from Alice to Bob and vice-versa. Otherwise, it is called unidirectional. In unidirectional PRE schemes, the proxy can only transform in one direction. Blaze et al. also gave another method to classify PRE schemes, called multiuse, i.e., the ciphertext can be transformed from Alice to Bob to Charlie and so on; and single-use, i.e., the ciphertext can be transformed only once. Due to its transformation property, PRE schemes can be used in many applications, including simplification of key distribution, key escrow, distributed file systems, multicast, anonymous communication, DFA-based FPRE system, and cloud computation. Recently, the research of cloud email system has become more and more popular in business and organizations as it allows an enterprise to rent the cloud SaaS service to build an email system with less costs and maintenance efforts. Indeed, it is much cheaper and scalable than traditional on premises solution. However, these solutions have a common drawback: the grant of content sharing capability, which is achieved through the generation of re-encryption key.

Up to now, in all of the traditional identity based proxy re-encryption schemes, the generation of re-encryption key is generally divided into two ways: in uni-directional proxy re-encryption scheme, the key is generated by an authorized person A; in bi-directional scheme, it is generated by A and the recipient B. Recently, Wang et al. proposed a new scheme for the re-encryption key generation, where the key is generated by the sender S. This way has the advantage that the sender S can control the authorization granting process by using the random number, which is used in the encryption process to generate the proxy re-encryption key.

In this work, we propose a new identity based proxy re-encryption system. In the new identity based proxy encryption system, the re-encryption key is generated by the sender S, and the process of agency is controlled by S thoroughly. This method can avoid the flaw of the traditional proxy re-encryption; the sender S can control the people who can get the message and the sharing content of the messages.

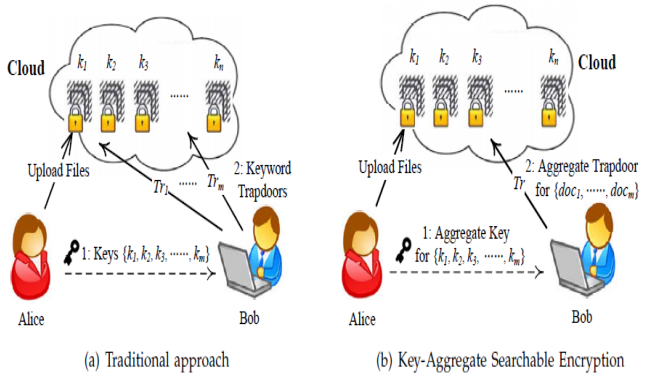

Fig.1 Secured Data Sharing over Cloud

The proposed scheme does not compute authentication values separately for a proof of the PoW process and for a proof of the integrity auditing; instead, it computes only one authentication value depending on the duplication. The proposed scheme uses the BLS signature based homomorphism authenticator to generate the authentication value to provide secure Deduplication and public integrity auditing. The user also generates (spk, ssk) to digitally sign a file using a

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

cryptographically secure signature scheme such as RSA PSS, or DSA. It is assumed that the public key is distributed securely to the entities.

In this system, based on Wang et al. 's proposal and 3-linear map introduced in earlier systems, we propose the IBPRE+ scheme by using identity based encryption and 3-linear map, and analyse the proposal's property. Toward this construction, we first review the Identity Based Encryption (IBE) scheme, and then we construct a new IBE scheme based on 3-linear Map. Based on that scheme, we propose our IBPRE+ scheme. We roughly discuss the properties of our IBPRE+ scheme. Finally, we demonstrate the potential application of our scheme to secure cloud data sharing. First upload procedure: In this case, a user first uploads a file that is not stored in the CSS. First, a file ID/Tag and a convergent encryption key K are generated, and the file is encrypted using CE with K and then uploaded to the CSS. The CSS maintains the list owner, tag, and ciphertext. The user computes an authentication tag for the integrity auditing and sends it to the TPA. Subsequent upload procedure: This procedure is performed when a duplicate file is uploaded. The CSS checks for the duplication using the file tag, and in the event of duplication, it proceeds with the PoW protocol to examine the ownership of the user. If a user passes this process, the CSS adds the file ownership of the user to the stored file. Integrity auditing procedure: Periodic auditing is required to ensure that the files stored on the CSS are fully and intently maintained. To reduce the user overhead, the TPA performs periodic integrity audits. To do this, the TPA first chooses a random challenge and it sends it to the CSS. The CSS responds by generating a corresponding proof using the stored file. Then the TPA verifies that the response is valid and completes the integrity audit.

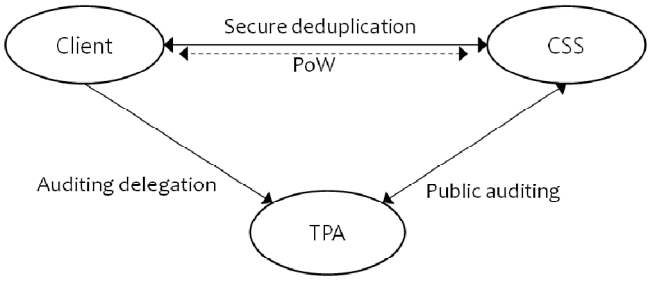

Fig.2. System Model

II. SYSTEM IMPLEMENTATION

A. CLOUD STORAGE AND SECURITY

Cloud storage has emerged as a promising solution for providing ubiquitous, convenient, and on-demand accesses to large amounts of data shared over the Internet. Today, millions of users are sharing personal data, such as photos and videos, with their friends through social network applications based on cloud storage on a daily basis. Business users are also being attracted by cloud storage due to its numerous benefits, including lower cost, greater agility, and better resource utilization.

However, while enjoying the convenience of sharing data via cloud storage, users are also increasingly concerned about inadvertent data leaks in the cloud. Such data leaks, caused by a malicious adversary or a misbehaving cloud operator, can usually lead to serious breaches of personal privacy or business secrets (e.g., the recent high profile incident of celebrity photos being leaked in iCloud). To address users' concerns over potential data leaks in cloud storage, a common approach is for the data owner to encrypt all the data before uploading them to the cloud, such that later the encrypted data may be retrieved and decrypted by those who have the decryption keys. Such a cloud storage is often called the cryptographic cloud storage. However, the encryption of data makes it challenging for users to search and then selectively retrieve only the data containing given keywords.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

A common solution is to employ a searchable encryption (SE) scheme in which the data owner is required to encrypt potential keywords and upload them to the cloud together with encrypted data, such that, for retrieving data matching a keyword, the user will send the corresponding keyword trapdoor to the cloud for performing search over the encrypted data. Although combining a searchable encryption scheme with cryptographic cloud storage can achieve the basic security requirements of a cloud storage, implementing such a system for large scale applications involving millions of users and billions of files may still be hindered by practical issues involving the efficient management of encryption keys, which, to the best of our knowledge, are largely ignored in the literature. First of all, the need for selectively sharing encrypted data with different users (e.g., sharing a photo with certain friends in a social network application, or sharing a business document with certain colleagues on a cloud drive) usually demands different encryption keys to be used for different files. However, this implies the number of keys that need to be distributed to users, both for them to search over the encrypted files and to decrypt the files, will be proportional to the number of such files. Such a large number of keys must not only be distributed to users via secure channels, but also be securely stored and managed by the users in their devices.

In addition, a large number of trapdoors must be generated by users and submitted to the cloud in order to perform a keyword search over many files. The implied need for secure communication, storage, and computational complexity may render such a system inefficient and impractical. In this paper, we address this challenge by proposing the novel concept of key-aggregate searchable encryption (KASE), and instantiating the concept through a concrete KASE scheme. The proposed KASE scheme applies to any cloud storage that supports the searchable group data sharing functionality, which means any user may selectively share a group of selected files with a group of selected users, while allowing the latter to perform keyword search over the former. To support searchable group data sharing the main requirements for efficient key management are twofold. First, a data owner only needs to distribute a single aggregate key (instead of a group of keys) to a user for sharing any number of files. Second, the user only needs to submit a single aggregate trapdoor (instead of a group of trapdoors) to the cloud for performing keyword search over any number of shared files. To the best of our knowledge, the KASE scheme proposed in this paper is the first known scheme that can satisfy both requirements (the key-aggregate cryptosystem, which has inspired our work, can satisfy the first requirement but not the second).

B. SYSTEM STUDY

Consider a scenario where two employees of a company would like to share some confidential business data using a public cloud storage service (e.g., dropbox or simplicity). For instance, Alice wants to upload a large collection of financial documents to the cloud storage, which are meant for the directors of different departments to review. Suppose those documents contain highly sensitive information that should only be accessed by authorized users, and Bob is one of the directors and is thus authorized to view documents related to his department. Due to concerns about potential data leakage in the cloud, Alice encrypts these documents with different keys, and generates keyword ciphertexts based on department names, before uploading to the cloud storage. Alice then uploads and shares those documents with the directors using the sharing functionality of the cloud storage.

In order for Bob to view the documents related to his department, Alice must delegate to Bob the rights both for keyword search over those documents, and for decryption of documents related to Bob's department. With a traditional approach, Alice must securely send all the searchable encryption keys to Bob. After receiving these keys, Bob must store them securely, and then he must generate all the keyword trapdoors using these keys in order to perform a keyword search. As shown in Fig.3(a), Al ce is assumed to have a private document set fdocigni =1, and for each document doci , a searchable encryption key ki is used. Without loss of generality, we suppose Alice wants to share m documents fdocigmi=1 with Bob. In this case, Alice must send all the searchable encryption keys fkigmi=1 to Bob. Then, when Bob wants to retrieve documents containing a keyword w, he must generate keyword trapdoor Tri for each document doci with key ki and submit all the trapdoors fTrigmi =1 to the cloud server. When m is sufficiently large, the key distribution and storage as well as the trapdoor generation may become too expensive for Bob's client-side device, which basically defies the purpose of using cloud storage.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

C. USER AUTHORIZATION AND AUTHENTICATION

Authentication is one of most popular and important factor to enter into the required portals and applications. This enhanced authentication norms module allows the user (Resource Owner/Resource User) to authenticate themselves into the system with proper identities such as Name, Mobile Number, E-Mail-Id, Address and so on. Once the authentication process is done, the users have specific rights to proceed into the application and access all the features present into it. The Enhanced Authentication Norms is derived based on two-factor authentication, which enables user to proceed with two-levels of authentication features such as Username and Password, High-Secure Key Generation process. For the entire authentication module is the pathway of all users to proceed into the system and accessing the features. Proxy defines the security by means of user authorization and authentication. Proxy signature is a signature scheme, in which an original signer can delegate his/her signing capability to a proxy signer, and then the proxy signer generates a signature on behalf of the original signer.

D. DATA MANIPULATION

The data manipulation module supports Resource Owner scenario and it allows the resource owner to maintain the data into the cloud server securely and wishes to upload it into the cloud storage to save costs. A resource owner encrypts the data and outsources it to the cloud storage with its index information, that is, a tag. If a resource owner uploads data that do not already exist in the cloud storage, he is called an initial Uploader; if the data already exist, called a subsequent uploader since this implies that other owners may have uploaded the same data previously, he is called a subsequent uploader. Hereafter, we refer to a set of resource owners who share the same data in the cloud storage as an ownership group. The Resource Owner can encrypt the data by using Identity Based Provable Re-Encryption methodology, which allows the data to be encrypted twice and provides highest security feature to the system.

E. DATA DEDUPLICATION SCHEME

This data Deduplication module allows the data owner to maintain the records into the server more dynamically and with full of integrity. Once the data owner uploaded the records into the database/server, which is counted and manipulated at every time while uploading the data next time into the server. If the data matches with the existing records, the system won't allow the data owner to upload the data further and blocks them to proceed.

F. CONTENT BASED DATA SEARCH

The Content Based Data Search module eliminates the problem of unwanted confusions and problems over data mining scenario, which is achieved by means of structured data maintenance module. The structured data storage scheme fully describes about the flow of data structure maintenance and the concept of implicit data mining and document maintenance schema. Once the resource owner uploads the respective document it checks for the reference schema of the existing document for reference, if the document is presented in the database server then the following document is sequenced under the existing document otherwise it creates a new schema for the following document, so that the data into the database server is maintained in the structured manner. All the data into the server is based on the cluster format and provides the frequent access for the user search between the server and the data client (user).

G. PAGE RANKING SCENARIO

The PageRank model is a ranking methodology used by Search engines to rank the resulting in their search results. PageRank is a way of measuring the importance of website pages. According to Google: PageRank works by counting the number and quality of links to a page to determine a rough estimate of how important the website is. The underlying assumption is that more important websites are likely to receive more links from other websites. It is not the only algorithm used by Google to order search engine results, but it is the first algorithm that was used by the company, and it is the best-known.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

III. LITERATURE SURVEY

Achieving Secure, Scalable, And Fine-Grained Data Access Control In Cloud Computing - S. Yu, C. Wang, K. Ren. [1] Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners.

To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secures under existing security models.

Secure Provenance: The Essential Of Bread And Butter Of Data Forensics In Cloud Computing - R. Lu, X. Lin. [2] Secure provenance that records ownership and process history of data objects is vital to the success of data forensics in cloud computing, yet it is still a challenging issue today. In this paper, to tackle this unexplored area in cloud computing, we proposed a new secure provenance scheme based on the bilinear pairing techniques. As the essential bread and butter of data forensics and post investigation in cloud computing, the proposed scheme is characterized by providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access, and provenance tracking on disputed documents. With the provable security techniques, we formally demonstrate the proposed scheme is secure in the standard model.

Mona: Secure Multiowner Data Sharing For Dynamic Groups In The Cloud - X. Liu, Y. Zhang. [3] With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, we propose a secure multi-owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

Practical Techniques For Searches On Encrypted Data - X. Song, D.Wagner. [4] It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query, without loss of data confidentiality. We describe our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms presented are simple, fast (for a document of length n, the encryption and search algorithms only need O(n) stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

Searchable Symmetric Encryption: Improved Definitions And Efficient Constructions - R. Curtmola, J. Garay. [5] Searchable symmetric encryption (SSE) allows a party to outsource the storage of its data to another party (a server) in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research in recent years. In this paper we show two solutions to SSE that simultaneously enjoy the following properties: Both solutions are more efficient than all previous constant-round schemes. In particular, the work performed by the server per returned document is constant as opposed to linear in the size of the data. Both solutions enjoy stronger security guarantees than previous constant-round schemes. In fact, we point out subtle but serious problems with previous notions of security for SSE, and show how to design constructions which avoid these pitfalls.

Further, our second solution also achieves what we call adaptive SSE security, where queries to the server can be chosen adaptively (by the adversary) during the execution of the search; this notion is both important in practice and has not been previously considered. Surprisingly, despite being more secure and more efficient, our SSE schemes are remarkably simple. We consider the simplicity of both solutions as an important step towards the deployment of SSE technologies. As an additional contribution, we also consider multi-user SSE.

Computationally Efficient Searchable Symmetric Encryption - P. Van,S. Sedghi. [6] Searchable encryption is a technique that allows a client to store documents on a server in encrypted form. Stored documents can be retrieved selectively while revealing as little information as possible to the server. In the symmetric searchable encryption domain, the storage and the retrieval are performed by the same client. Most conventional searchable encryption schemes suffer from two disadvantages. First, searching the stored documents takes time linear in the size of the database, and/or uses heavy arithmetic operations. Secondly, the existing schemes do not consider adaptive attackers; a search-query will reveal information even about documents stored in the future. If they do consider this, it is at a significant cost to the performance of updates. In this paper we propose a novel symmetric searchable encryption scheme that offers searching at constant time in the number of unique keywords stored on the server. We present two variants of the basic scheme which differ in the efficiency of search and storage. We show how each scheme could be used in a personal health record system.

IV. SYSTEM ANALYSIS

A. Existing System

Many cloud storage auditing schemes have been proposed up to now. These schemes consider several different aspects of cloud storage auditing such as the data dynamic update the privacy protection of user's data the data sharing among multiple clients and the multi-copies of cloud data. Key-exposure resilience, as another important aspect, has been proposed recently. Indeed, the secret key might be exposed due to the weak security sense and/or the low security settings of the client. Once a malicious cloud gets the client's secret key for cloud storage auditing, it can hide the data loss incidents by forging the authenticators of fake data.

DISADVANTAGES OF EXISTING SYSTEM

(a) Lack of Data Security
(b) Missing Data Integrity
(c) Trust Failure nature in maintenance
(d) Complex and Slow Retrieval Process

B. Proposed System

In the proposed system, we investigate how to preserve the security of cloud storage auditing scheme in any time period other than the key-exposure time period when the key exposure happens. We propose a paradigm named Identity Based Proxy Re-encryption Scheme with intelligent deduplication scheme called Deduplication Elimination Algorithm to provide highest flexibility to users to work with the cloud environment. The proposed system is used as a practical solution for the earlier mentioned problems in the cloud server system. We design a concrete Identity Based

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

Deduplication free resilient auditing scheme for secure cloud storage. A novel and efficient key update technique is used in the designed scheme. We formalize the definition and the security model of this new paradigm. In the security model, we consider the most powerful adversary who can query the secret keys of the client in all except one unexposed time period. The main advantage of the proposed system is TPA can only manage the server, not interrupt with data, because system dynamically checks all without manual intervention to avoid corruptions. We formalize the definition and the security model of this new paradigm. In the security model, we consider the most powerful adversary who can query the secret keys of the client in all except one unexposed time period.

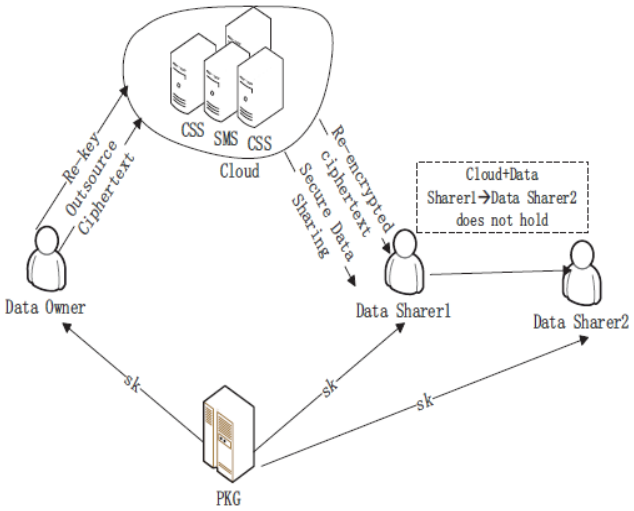

Fig.3 Proposed System Architecture Design

ADVANTAGES OF PROPOSED SYSTEM

(a) Despite of the various advantages of cloud services, outsourcing sensitive information such as e-mails, personal health records, company finance data, government documents, etc.
(b) High Speed and Exact Data Retrieval.
(c) Performance is good.

V. RESULTS AND DISCUSSION

In this section, we provided the simulated results of entire project with its practical proofs. The following figure shows the Home Page of the Proposed System.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

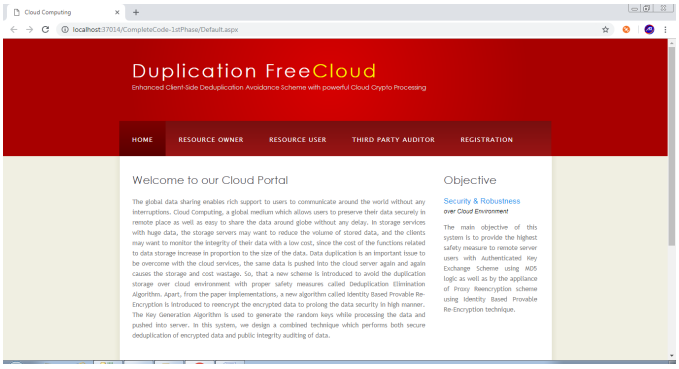

Fig.4 Home Page

The following figure illustrates the Registration view of the proposed system.

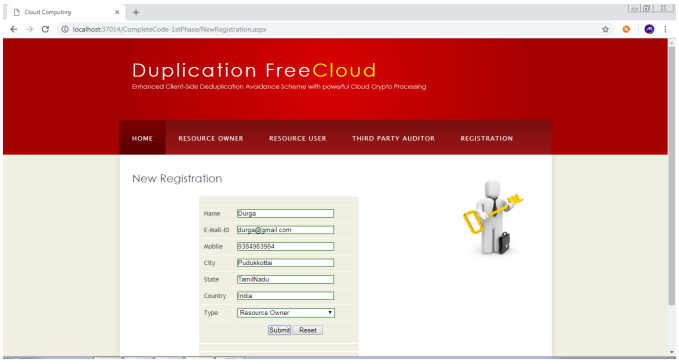

Fig.5 Registration

The following figure illustrates the CSP Authentication view of the proposed system.

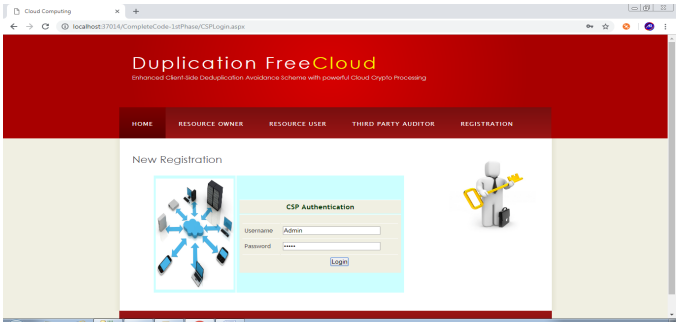

Fig.6 CSP Authentication

VI. CONCLUSION

When storing data on remote cloud storages, users want to be assured that their outsourced data are maintained accurately in the remote storage without being corrupted. In addition, cloud servers want to use their storage more

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

efficiently and to satisfy both the requirements, we proposed a scheme to achieve both secure Deduplication and integrity auditing in a cloud environment. To prevent leakage of important information about user data, the proposed scheme supports a client-side Deduplication of encrypted data, while simultaneously supporting public auditing of encrypted data. The proposed scheme satisfied the security objectives and improved the problems of the existing schemes. In addition, it provides better efficiency than the existing schemes in the viewpoint of client-side computational overhead and finally we designed two variations for higher security and better performance. The first variance guarantees higher security in the sense that a legitimate user can be an adversary. The second variance provides better performance from the perspective of the clients, by permitting low-powered clients to perform upload procedure very efficiently by passing on their costly operations to the CSS.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of the 14th ACM conference on Computer and communications security (CCS'07), Alexandria, Virginia, USA, 2007, pp. 598–609.
[2] G. Ateniese, R. Di Pietro, L.V. Mancini and G. Tsudik, "Scalable and efficient provable data possession," in Proc. of the 4th international conference on Security and privacy in communication netowrks (SecureComm'08), Istanbul, Turkey, 2008, pp. 1–10.
[3] D. Boneh, B. Lynn and H. Shacham, "Short signatures from the Weil pairing," Journal of Cryptology, vol. 17, no. 4, pp. 297–319, Sept. 2004.
[4] Y. Dodis, S. Vadhan and D. Wichs, "Proofs of retrievability via hardness amplification," in Proc. of the 6th Theory of Cryptography Conference on Theory of Cryptography (TCC'09), San Francisco, CA, USA, 2009, pp. 109–127.
[5] M. Dworkin, "Recommendation for block cipher modes of operation. methods and techniques," NIST, USA, No. NIST-SP-800-38A., 2001.
[6] C. Erway, A. Küpçü, C. Papamanthou and R. Tamassia, "Dynamic provable data possession," in Proc. of the 16th ACM conference on Computer and communications security (CCS'09), Chicago, Illinois, USA, 2009, pp. 213–222.
[7] J. Gantz and D. Reinsel, "The digital universe decade - are you ready?," IDC White Paper, 2010.
[8] S. Halevi, D. Harnik and B. Pinkas and A. Shulman-Peleg, "Proofs of ownership in remote storage systems," in Proc. of the 18th ACM conference on Computer and communications security (CCS'11), Chicago, USA, 2011, pp. 491–500.
[9] D. Harnik, B. Pinkas and A. Shulman-Peleg, "Side channels in cloud services: Deduplication in cloud storage," IEEE Security & Privacy, vol. 8, no. 6, pp. 40–47, Dec. 2010.
[10] A. Juels and B.S. Kaliski Jr, "Pors: proofs of retrievability for large files," in Proc. of the 14th ACM conference on Computer and communications security (CCS'07), Alexandria, Virginia, USA, 2007, pp. 584–597.
[11] S. Keelveedhi and M. Bellare and T. Ristenpart, "DupLESS: serveraided encryption for deduplicated storage," in Proc. of the 22nd USENIX Security Symposium (USENIX Security 13), Washington, D.C. USA, 2013, pp. 179–194.
[12] J. Li, J. Li, D. Xie and Z. Cai, "Secure auditing and deduplicating data in cloud," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2386–2396, Aug. 2016.
[13] X. Liu,W. Sun, H. Quan,W. Lou, Y. Zhang and H. Li, "Publicly verifiable inner product evaluation over outsourced data streams under multiple keys," IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 826-838, Sept.-Oct. 2017.
[14] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of the 14th International Conference on the Theory and Application of Cryptology and Information Security, Advances in Cryptology - ASIACRYPT 2008, Melbourne, Australia, 2008, pp. 90–107.
[15] Q.Wang, C.Wang, K. Ren,W. Lou and 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, Dec. 2011.
[16] T. Y. Youn, K. Y. Chang, K. R. Rhee and S. U. Shin, "Public Audit and Secure Deduplication in Cloud Storage using BLS signature," Research Briefs on Informaiton & Communication Technology Evolution (ReBICTE), vol. 3, article no. 14, pp. 1-10, Nov. 2017.
[17] J. Yuan and S. Yu, "Proofs of retrievability with public verifiability and constant communication cost in cloud," in Proc. of the 2013 international workshop on Security in cloud computing, Hangzhou, China, 2013, pp. 19–26.
[18] J. Yuan and S. Yu, "Secure and constant cost public cloud storage auditing with deduplication," in Communications and Network Security (CNS), 2013 IEEE Conference on, National Harbor, MD, USA, 2013, pp. 145-153.