An Approach to Zero Knowledge Proof for Secure Data Sharing in Cloud Storage: New Direction

Amjan Shaik, B. Madhurima, M. Neelakantappa

Abstract**:** ***Now a days, Cloud computing (CC) is seriously growing because of it's strengths like elastic, flexible, on-demand storage and fast computing services for users. In cloud based storage concept, data owner does not have full control over own data because data controlled by the third party called cloud service providers (CSP). The most challenging issue in data security arises when the owner of the data shares to other through cloud. This issue is very common as data is shared in the cloud computing environment. This issue is addressed by few researchers through encryption techniques of cryptography to provide secure data-sharing on the cloud. In this paper, we propose a model to provide security of shared data on cloud in terms of access control and data confidentiality. This system eliminates the need of key management and file encryptions and descriptions by the users. It also supports dynamic changes of user permissions (Read,Write), there by removes the need of owner to be always online during user accessing of data from cloud. In this system, we extended the notion of zero-knowledge proofs of the membership (that reveals 1 bit of information) to zero-knowledge proofs of the knowledge(that reveals no information at all). The common weakness of conventional communication protocols is they are vulnerable to the impersonation attacks. Each time this type of protocol is executed, the system degrades due to the threat of an eavas-dropper listening the communication. The main objective of this designed system is that it makes possible for a prover for convincing a verifier of his knowledge of a certain secret without revealing any information apart from validity of his claim.***

Keywords: Cloud computing, cloud storage, Data security, cloud service provider, secure sharing, cryptography.

I. INTRODUCTION

In this era, technically cloud is nothing but a software program/application/service/r an entire infrastructure. The cloud is a term referring to accessing computer, information technology (IT), and software applications through a network connection, often by accessing data centers using wide area networking (WAN) or Internet connectivity.

1.1 Cloud computing

It's often quicker in provision of the service and most commonly service can be accessed instantly. Remote users can avail access to cloud-resources from their place, where they have a connection rather than being limited by their geographical location. Cloud computing have many advantages: Self-service provisioning, elasticity, pay-per-use, work-load resilience and migration flexibility. The deployment models of cloud computing services can be divided into three groups: private, public and hybrid, with reference to whom accessing of services or infrastructure is provided.

Public cloud services are designed to provide access to everybody, who purchases or take lease of the services. Private-cloud services are developed by enterprises for use specifically by their employees & their collaboration-partners. Hybrid cloud service will combine these two services.

1.2Cloud storage:

Cloud storage refers to a service model by which data in managed, maintained and backed remotely so that data is made always available to users over the internetwork. Generally, users will pay for their cloud data storage on the basis on consumption on a monthly basis. Even though the storage cost (per giga byte)has been drastically reduced, cloud storage provides need to meet operating expenses which makes the system more expensive compared to payment by the users. For users, cloud security is big concerns which were addressed by provides by developing security capabilities in the form of authentication and encryptions into their cloud services.

Cloud storage is an application of clouds which liberates the companies from establishment of in house data storage systems. However, cloud storage continues to be a security concern. Generally, for shared-group, the data is vulnerable to cloud specific & conventional insider specific in terms of threats. Data sharing in a secured way among the group, which counters insider threats by malicious users, is the most challenging research issue.

This paper deals with proposal of secured data sharing in cloud (SDSC) model which presents 1.Data-integrity & confidentiality 2.Access-control 3.Data-sharing (transmission) without use of re-encryption computing 4.Insider threat security 5. Forward & backward access control. This SDSC system will encryption key. Two different key shares re generated to each user with this methodology, each user gets only one share, through which SDSC technique counters, the insider threat. The other key-share is stored by a trusted third-party, referred to as crypto-graphic server. For data sharing, privacy and security in the applicable to both conventional &mobile cloud-computing environments.

Revised Manuscript Received on December 28, 2018.

Sudhamani M J, RNS Institute of Technology, Bengaluru, Karanataka, India.

M K Venkatesha, RNS Institute of Technology, Bengaluru, Karnataka, India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

1.3 Data security

Data security deals with protective-privacy measures, which are applied for preventing un-authorized accessing of computers, websites and data-bases. It also refers to protection of data from corruption. Data security is an important element of IT for companies of any size and type .It is also referred as computer security or information security.

1.3.1 Examples of Data Security

The Data security techniques include back-ups, data era sure and data masking. The main data security technique in is encryption, by which digital data, software and hard-drives can be encrypted and hence these are un-readable for un-authorized users or hackers.

The most common technique of data security practice is the application of authentication through authentication; users have to be provided by a password, code, bio-metric data or any other form of data for verifying the user identity before granting access to the data or system.

Data security had a significant role in the health-care record, so that the medical practices and health advocates in U.S are working hard to implement electronic-medical-record (EMR) privacy to create awareness on patient rights with reference to data released to the labs, hospitals, physicians and other medical resources.

1.4 Cloud service provider (CSP)

CSP is an organization which offers functionality of cloud computing to other companies or individuals covering Saas (software as a service), Iaas (Information as a service) or Paas (platform as a service).

1.4.1 Major cloud service providers

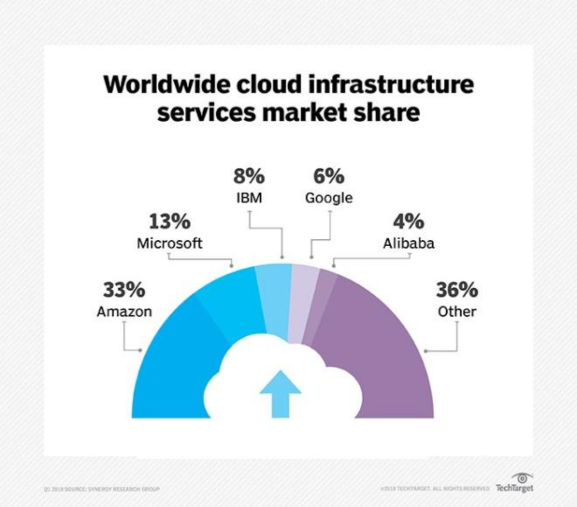


Figure.1: Market Share of Cloud Infrastructure Services

As shown in the Figure1, the market of cloud-services had wide range of providers, but four companies have built up themselves as dominant forces Google, Amazon Web Services (AWS), IBM, and IBM Microsoft.

1.4.2 Secure Sharing

It is the process by which user can share one or multiple files privately and securely. Secure sharing facilitates different organizations, users to share files confidentially in a protected mode so that they secured from un-authorized users or intruders. There- fore secure file sharing is also referred to as protected file sharing.

1.5 Cryptography

Cryptography is the process through which plain text can be converted into cipher text and vice versa using public/private key. This technique is used to store and transmit data in a specific form, so that only those users can access than to read or process it. Cryptography also provides user authentication apart from data protection .Initially cryptography was basically process of encryption and decryption but now-a-days it is mostly based upon combination of mathematical theory & computer Science approaches.

1.5.1 Modern cryptography Elements:

Confidentiality – Information should not be accepted or understand to others.

Integrity – Information should not be altered (modified).

Non-repudiation – Sender/Receiver cannot deny his/her transmitted/ received information in later stage

Authentication – Sender & receiver have to confirm each other.

1.5.2 Applications of Cryptography

Cryptography can be used for many applications such as e-commerce transactions, computer passwords, online banking applications etc.

Generally, three types of cryptographic methods can be used.

1. Symmetric-key cryptography
2. Public key cryptography
3. Hash functions

Symmetric Key Cryptography: In this type of cryptography, the sender & receiver agrees upon sharing a single key. The sender encrypts the message using this key and transmits resulted cipher text to the receiver. At the other-side, the receiver decrypts the cipher text by using the same key to get back the message (plain text).

Public Key Cryptography: This technique of cryptography is the most revolutionary topic for the last 30-40 years. In this approach, 2 related keys referred as public key & private key are used. Public-key can be distributed, but its paired private will be kept secret using the public key, the message can be encrypted by anybody and which can be decrypted by any the intended users, who has that corresponding private-key.

Hash Functions: In this approach no key is required. As per the plain-text, a fixed length hash value is computed which makes impossible to recover the plain text. Hash functions can also be used by operating-systems for encrypting the passwords.

Access Control: This security concept related to the regulation of the user, who and what can be viewed or use the resources in a computing system. Access control techniques can be categorized into two types known as physical and logical. The physical access control will limit the access to buildings, rooms and It assets physically, logical access will limit the connection to computer-network, data & system files. The main functionalities of access control include authentication, authorization, access approval and accountability of the entities. These functionalities of the access control mechanism can be done through login credentials, which include passwords, biometric scans, PINs (personal Identification Number) and electronic keys.

II. RESEARCH BACKGROUND

The key contributions towards proof of ownership are illustrated as follows.

2.1 Proofs of ownership:

In this paper Halevi[1] presented the notation for “proof of ownership” by which the deduplication systems like a client will technically prove to the cloud storage server that it owns that file without up-loading the file. Proof of ownership (pow) constructions are based on the mark’s Hash tree, which are proposed in the paper [1] for enhancing the client side deduplication, that contains the bonded leak setting. In their paper pietro&sorniotti[2] presented an efficient pow scheme, which allows to choose the projection of a file onto few random chooses bit positions as the proof of the file. But these proposals will not consider data privacy, In another paper Nget [3] extended the pow for files which are encrypted but it has disadvantages of overhead in key management process.In paper [4], Fiat and Shamir proposed some simple signature and identification schemes that enable all users for proving their identity and authenticity of their messages for other users without public or shared keys. This scheme is probably secure against any selected message attack if factoring is complex and specific implementations need only 1% to 5% of the number of multiplications needed by the RSA cryptographic technique, with the advantage of their simplicity, speed and security, these techniques are ideally suits micro-processor based devices like pcs, smart cards and remote control schemes.In paper [5], Seo has proposed themediated- certificate -less encryption technique that reduces the computational overhead in regard to bilinear pairing. This approach enables data sharing in the public cloud without using bilinear pairing. In this proposal, the cloud will generate public and private key pairs for every used and sends the public keys for each contributing user. The decryption will be done partially at the cloud. As partial decryption and key management have done by cloud, user revocation can be handled easily. But this proposed treats the public cloud both as trusted and un-trusted system. Based on technique of shared-key derivation, chen&tzeng proposed a mechanism in the paper [6] for data security in a group. This technique applies a binary tree for generating the keys. But this proposed mechanism has high computational cost as the re-keying technique is employed heavily. Also, this mechanism may poor customized for systems of public-cloud. Familier mechanism is also proposed in RSA algorithm [7] by Rivest, Shamir and Adleman.

2.2 Existing Problem and Proposed Mechanism

Data sharing is facing many security issues such as security of data, unauthorized users, Insider threats, lack of security on the third party (cryptosystem).Proposed Contribution: To overcome the drawbacks of the existing methods as specified above, we designed a new technique known as “Zero knowledge proof”.In this paper, we are presenting the Zero Knowledge Protocols (ZKP) Goldwasser [8].The basic idea of ZKP protocol is proposed by Goldreich in his paper [9], designed for defecting the drawbacks as specified above. In this ZKP protocol, the prover tries to demonstrate the information of a specific secret to the verifier. The key intention, of this protocol is to get proof without revealing any information of the proof except the valid one.ZKP proofs have to be compared with the answer expected from the trusted party.It is clear that the mechanism in ZKP is quite different from the conventional mathematics concepts. The proofs by mathematics are rigid, which applies either self-evident statements or statement derived from the proofs established before hard. ZK proofs works by the dynamic process applied by humans for establishing the truth for a statement through of the information exchange session. Instead of relying on a static proof for a statement, ZKP allows prover to involve the verifier to interactively convince him in regard to the truth of the statement.In ZKP, there are two parties existing in proof derivation.

i) Data Owner, the prover: The data owner needs to convey the proof of certain knowledge to the consultancy system (CS) without revealing the secret information.

ii) CS, the verifier: CS poses the data owner a series of queries to decide whether which he claims to know. This process will not allow deducing any secret information from the data owner through this interaction even if CS tries to cheat or influence the activities outside the protocol.

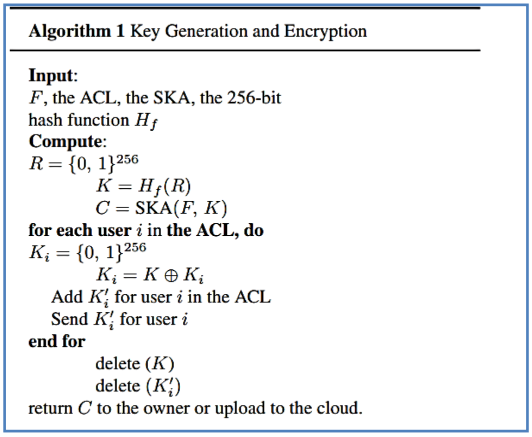
III. METHODOLOGY

In order to achieve security goals, the cryptographic-key operations are here presented in this section.

3.1 Algorithms in Proposed System

3.1.1 Algorithm 1- Key generation and Encryption

Encryption refers to conversion of plain text message into cipher text, and key generating Process.



```
Algorithm 1 Key Generation and Encryption

Input:
$F$, the ACL, the SKA, the 256-bit
hash function $H_f$
Compute:
$R = \{0, 1\}^{256}$
          $K = H_f(R)$
          $C = \mathrm{SKA}(F, K)$
for each user $i$ in the ACL, do
$K_i = \{0, 1\}^{256}$
          $K_i = K \oplus K_i$
    Add $K_i'$ for user $i$ in the ACL
    Send $K_i'$ for user $i$
end for
          delete $(K)$
          delete $(K_i')$
return $C$ to the owner or upload to the cloud.
```

Figure 2: Algorithm 1- Key generation & Encryption [10]

File Encryption: Generally, depends on needy, to share data among the group, the owner of the data sends the request for encryption to the CS. This request encompasses with file F & list L of all the users, which here got access permission to that file F. The list L will also consists of the access right of all users.

In general, the users can have access permissions such as READ-only and/or READ-WRITE to that file. For enforcing file grained access control over the file, other parameters can also be set. To generate ACL for that data, L is used by the CS. The list L is transmitted to the CS only when there is a data to be shared exist (may exist already), this request for encryption can not contain instead, group-ID of existing encryption request, the CS generates the ACL for each file, the ACL is maintained separately. The ACL consists of information of the file like file ID, owner ID, size, and the list of users ID for whom file being shared and meta-data. In case of the existing groups, only ACL of the file is generated. Thereafter, the CS will generate K according to the defined process and encrypts that file with an appropriate symmetric block-cipher. For our proposed system, AES encryption technique is used. .

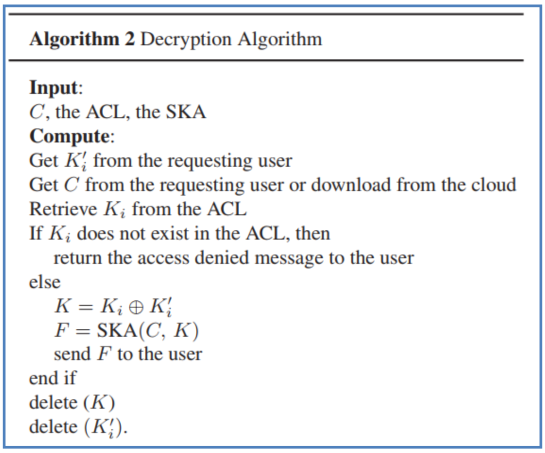
The encrypted file (C) is the result of the above process. Next, the CS   creates Ki and Ki for each user and using secure overwriting concepts, memory bits will constantly flipped for making sure that, the memory-cell will not grip a charge for a period, duration which it has to be remembered or re covered. The ACL is inserted with Ki of each user. For maintaining file's, integrity, CS will generates hash-based message authenticated code signature (HMAC) for each file encrypted.A similar process in adopted to generate HMAC-key. But the HMAC-key will remains with CS only and will not be disturbed. The encrypted data along with the group ID and the Ki for the owner are sent to the requested data owner. Group ID and Ki for n owner, will be send to the requested data-owner.

This group ID and Ki for the remaining group-users, will be sent directly to through a secured communication-channel. The group users public-keys can be utilised for transmitting the user position of the key. In this method, the public-keys of these users are needed for transmitting the key-positions, after arrival of C, the users up-loads it onto the cloud. After uploading, K will be deleted through secure over-writing process by the CS.

Algorithm-1 presents the key-generation & encryption-process at the CS end. The notable point in this process is that, the key-generation process is executed only after the initiation of the groups and submission of the first file the encryption. Also, a new user joined in that group also activates key-generation process only for himself.

3.2 Algorithm 2- Decryption Algorithm

Decryption is the process of Converting the cipher text back to the plain text.



```
Algorithm 2 Decryption Algorithm

Input:
$C$, the ACL, the SKA
Compute:
Get $K_i'$ from the requesting user
Get $C$ from the requesting user or download from the cloud
Retrieve $K_i$ from the ACL
If $K_i$ does not exist in the ACL, then
    return the access denied message to the user
else
    $K = K_i \oplus K_i'$
    $F = \mathrm{SKA}(C, K)$
    send $F$ to the user
end if
delete ($K$)
delete ($K_i'$).
```

Figure 3: Algorithm 2- Decryption Process [10]

File Decryption: The authorized user sends to the CS with a request of download or themselves download the encrypted-file (C) from this cloud & sends to this CS with the decryption-request of the locally maintained ACL, this cloud checks the authorization-rights of that user. The decryption request will accompany the user portion of the key, Ki, in addition to other authentication credentials. The CS generates K with the application of EX-OR operation the Ki over the corresponding Ki from the ACL. As every user referred to a distinct pair of Ki and Ki, no users can use other Ki for primary identity. After verification of the integrity of the file, the CS proceeds further in the decryption process. Incase if CS receives, the correct Ki then decryption process will be successful, and otherwise the decryption process will fail. Successful decryption leads to transmission of that file to requested-user via a secured communication-channel, such as SSL (Secure-Sockets-Layer) or IP sec (Internet-Protocol- Security) channels. Subsequently K will be deleted through secure over-writing at the CS. According to standard procedures, the users will be authenticated before the processing of their request. In Algorithm the decryption procedure is presented which is illustrated in Figure 3.

3.3 Algorithm 3: Zero-Knowledge Proof

In cryptography, a zero-knowledge proof is a technique through which one party (the prover) can prove to the other party (the verifier Victor) that he knows a value x, without conveying any other information other than the fact that he knows value x. If proving the statement needs knowledge of the proven-part, then this definition indicates that, this verifier cannot prove the given statement in-turn for any one else, as the secret information is unavailable to the verifier. Here, the noticeable point is that the statement to be proved should contain the assertion that the prover contains that knowledge. If not, this statement could't be proved in zero knowledge, as the verifier can get additional information about the knowledge needed for secret information, at the end of the protocol.In case of the statement containing only fact, that the prover holds the secret information, then that will be special-case referred as zero knowledge-proof, which presents the need notion of zero knowledge of particular information is trivial, if he is permitted for simply reveal this information. Un disturbly, the major challenge is prove, one-party contains that secret- information.For zero knowledge proofs, the mechanism should essentially need interactive information from the verifier, generally in a challenge from, which prover responses will convince the verifier if and only if the statement is true. This one is that the prover contains the knowledge, which he claims. Otherwise, the protocol execution can be recorded by the verifier, which reveals the secret information.In case that was agreed by new-party as the proof, that the re-playing party known about the secret-information, then the new-party's acceptance can be justified. About the re-player knows this secret-information, that means this protocol reveals the knowledge and hence it is not zero knowledge-proof or that can be is spurious, that is leading to a party to accept other's proof of knowledge, who didn't have that secret information.

3.3.1 Mathematical Equations:

In general cryptographical terms, let us assume, "Alice" desires to prove that "Bob" knows a value x, such that-

f(x) (mod) P=Y ------------- 1

In the above equation, f is a chosen value, P is a prime number and Y is a result. Even though Alice and Bob knows these values, it is complex to know the x value, as there are more x values which satisfies the above equation ------1

The prover Bob, has to prove himself about he knows x value, he will generate a random number r and sends the computed result to Alice:

C= fr (mod) P -------------- 2

Then he transmits

Cipher-1 = [f(x +r) (mod) (P−1)] (mod)P -----3

Next, Alice will computes

Cipher-2 = C.Y (mod) P --------- 4

In case, Cipher-1 equals to Cipher-2, then Bob has proven himself that, he knows this secret , which is x.

IV. SYSTEM ARCHITECTURE

This section, will presents our designed protocol, which secures the sharing & forwarding of information among group members without involvement of re-encryption in the given cloud environment.

4.1 Proposed System Architecture

This will show you, the data is shared between the users by providing the keys by CS, and the files are uploaded to the cloud by proving and checking the challenge value of CS.

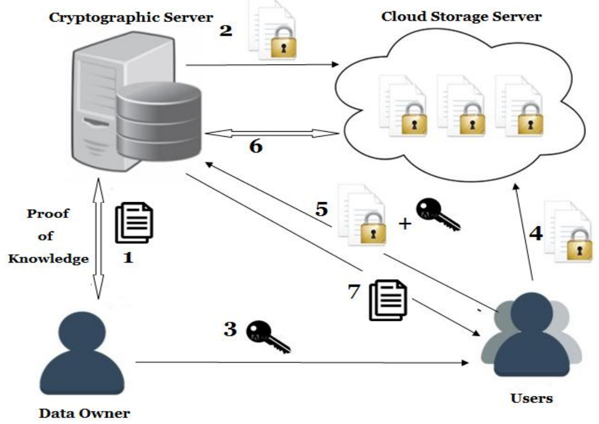


Figure 4: System Architecture

Cloud Storage Server: User gets storage services from the cloud, therefore, the information existing on the cloud need to be secured against privacy constraints. The data confidentiality must be ensured through storage of encrypted data on the cloud. The cloud mechanism involves only basic cloud-operations of the file up-loading and downloading. Hence, on the cloud there will not be any changes at the protocol level or implement level are required.Cryptographic Server: The Cryptographic Server (CS) is a trusted-party, which takes the responsibility in secured operations, like encryption, decryption, key-management, the ACL management to ensure confidentiality and data-forwarding among users of the group in a secured way. To get these security services, the users of the group of sharing data have to be registered with the CS. In our proposed mechanism, the CS is deemed to be a secured system. The CS has to be managed by a given organization or it has to be owned and managed by a third party. But , among these options, the CS managed by the organization will gets more trust in the group.Data Owner and Users: The clients of the storage cloud are its users. For a given data-file, one of the user will be the file-owner and the other group members will be the data-consumers. The file owner, sets the access-rights for the members of the group. In this way the access-rights of a file are created and can be revoked based on the file owner's decision. The CS manages the access rights in the ACL file format. For every data-file in the CS, a separate ACL file will be maintained.Departing Group User: The group owners has to notify the CS about its departing group member. This enables the CS remove all the records correspond to the departing user from the related files of the ACLs. Since the whole-key is not contained by the group members, the departed member can not decrypt any of the data-files belonging to the group. Therefore, the presence of encrypted-files, with a malicious departed member can not affect the security/privacy of the data. This is due to fact that, the malicious departed member will not be able to generate the whole key for the decryption. Hence, this technology also ensures the forward access control. The following section presents the methodology yielding about various security services.

V. RESULTS AND ANALYSIS

The experimental results for distribution of cloud data storage at various authorities on the real time data is depicted in the Figure 5.

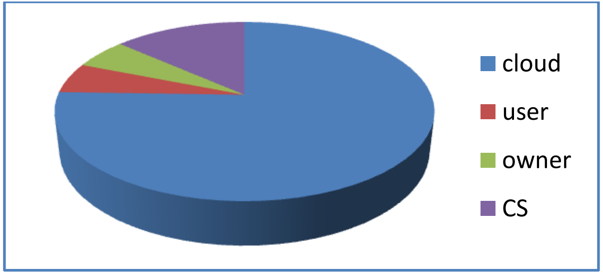


Figure 5: Cloud Data Storage Distribution

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

5.1 Privileges Authorized Data

The Figure 5 shows the portions of authorized access of data on cloud indicating their privileges.

Cloud: It stores the Data, and it also provides security to the data. It occupies the more portion of the storage, as it will be shared among users.

User: Users can view, edit and download a file.

Owner: They can upload, and also can revoke the users.

Cryptography System (CS): The CS will encrypt and decrypt the data, and provides the task of Key management.

5.2 AUTHORIZED ACTION PERFORMANCE

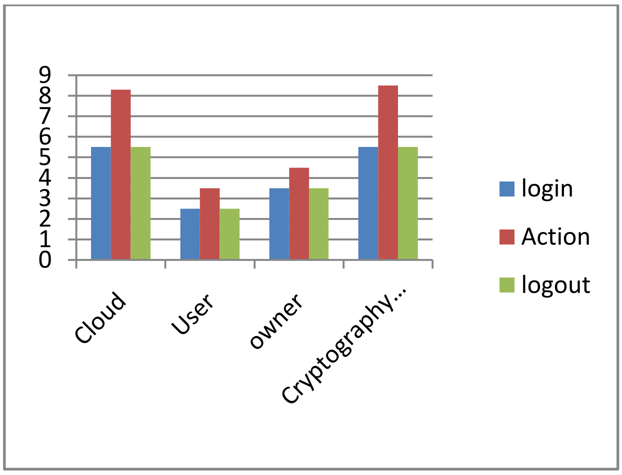


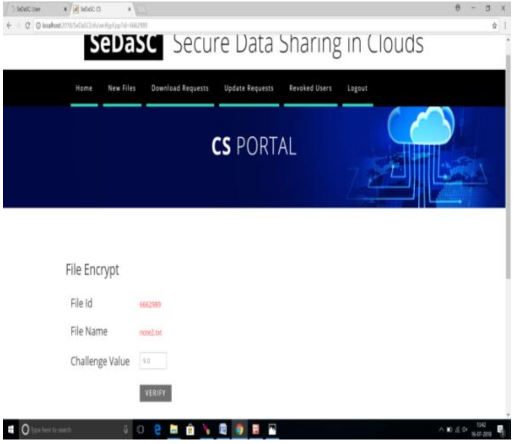
Figure 6: Action Performance by Individual Modules

Figure 6 indicates action performed by each module, in a tested cloud environment, where if it is authorized and trust worthy then only will get the access permission to perform the future process. For the tested instance, the cryptographic System (CS) has got highest contribution on number of actions by a module along with Cloud module, which is very high compared with user and owner modules. In cloud security, CS plays major role in authorizing the permissions to different kind of users/ owners which leads to high number of actions performed it.

5.3 Login Details and Key Management:

The Table 1gives the information of the login details of each module, access permission to upload/download, key management and storage permissions.

Screen Shot 1:- Before uploading a file verifying the



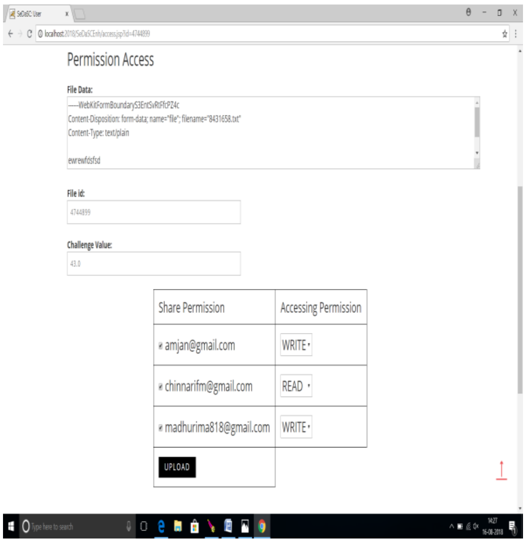
File Encrypt

File Id 6662989

File Name note2.txt

Challenge Value 9.0

Screen Shot 2: Read/Write Acess Permission before uploading a file.



Permission Access

File Data:

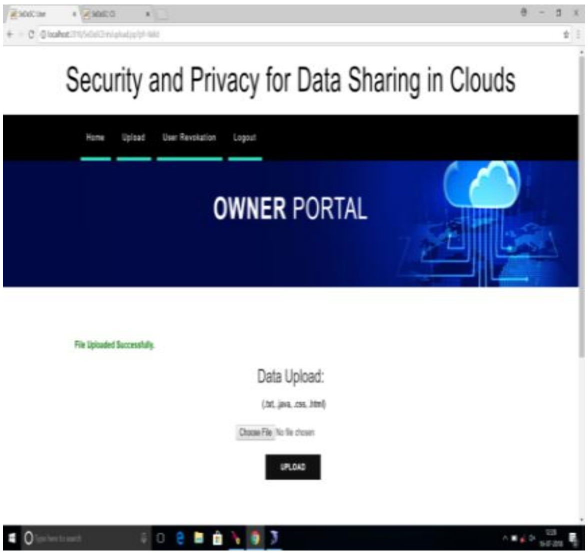
```
------WebKitFormBoundaryS3EntSvRtFfcPZ4c
Content-Disposition: form-data; name="file"; filename="8431658.txt"
Content-Type: text/plain

ewrewfdsfsd
```

File id: 4744899

Challenge Value: 43.0

Share Permission	Accessing Permission
☑ amjan@gmail.com	WRITE
☑ chinnarifm@gmail.com	READ
☑ madhurima818@gmail.com	WRITE

Screen Shot 3: Uploaded a file successfully CS whether it is trusted or not.



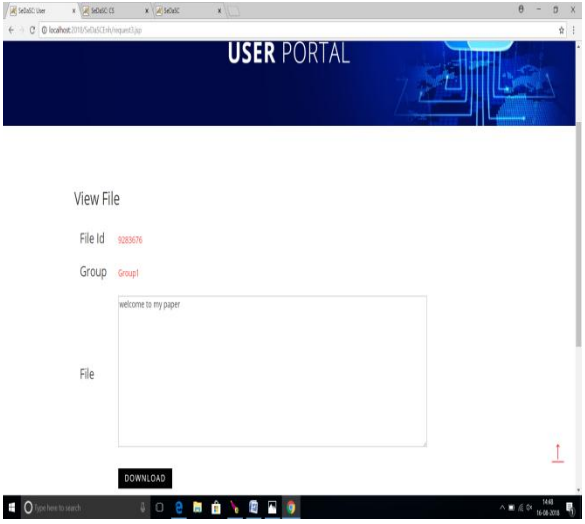
File Uploaded Successfully.

Data Upload:

(.txt, .java, .css, .html)

No file chosen

Screen Shot 4: Downloading a file.



View File

File Id 9283676

Group Group1

File welcome to my paper

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Table 1: Login Details and Key Management

Module	Name	Register/ login	Upload/ Download	Revoke users	Encryption/Decryption Key management	Stored files
Owner	Madhu	Login Success	Upload	Can Revoke	Verify challenge value of CS	_
		Login fail	No access	-		
User	Amjan	Login success	Download	_	_	After download
		Login fail	_		_	
CS	CS	Login success	_	_	Enc/dec, key generating and prover	_
		Login fail			_	
Cloud	Cloud	Login Success	_	_	_	Encrypted data can stored
		Login fail				

VI. CONCLUSION

The safety of cloud-storage services, is strongly geared to steadiness and consistency has both hypothetical research and practical significances. Here in this work, we proposed a zero-knowledge based protocol for group data sharing in cloud- storage. Using this protocol the data owner they can first verify the valid prover (CS) for performing cryptography techniques on given file resources. As well as using secure channel data owner can share the keys to data users for accessing the cloud data. Therefore none of any attacker does not know complete key for accessing cloud storage files.

In the future, there is a scope of including or implementing even on mobile cloud computing or cloud app for better results. It is very efficient, and concern about cost efficient too.

Reduce the time (consumption) where the workflow gets delayed. It's better to maintain a figure out of actions are like number of downloads, views, edited files. So that we can make sure of that and can more focus on the security issues.

ACKNOWLEDGMENT

We would like to thank the all the Authors in the Reference list and also thankful to the faculty, Department of CSE and IT to do this work in a better way.

REFERENCES

1. S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg.Proofs of ownership in remote storage systems. In Y. Chen, G. Danezis, and V. Shmatikov, editors, ACM Conference on Computer and Communications Security, pages 491–500. ACM, 2011.
2. R. D. Pietro and A. Sorniotti. Boosting efficiency and security in proof of ownership for deduplication. In H. Y. Youm and Y. Won, editors, ACM Symposium on Information, Computer and Communications Security, pages 81–82. ACM, 2012.
3. W. K. Ng, Y. Wen, and H. Zhu. Private data deduplication protocols in cloud storage. In S. Ossowski and P. Lecca, editors, Proceedings of the 27th Annual ACM Symposium on Applied Computing, pages 441–446. ACM, 2012.
4. Fiat, A. and A. Shamir, "HOW To Prove Yourself:Practical Solutions to Identification and Signature Problems", Proceedings of CRYPT0 1986.
5. S. Seo, M. Nabeel, X. Ding, and E. Bertino, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds," IEEE Trans.Knowl. Data Eng., vol. 26, no. 9, pp. 2107–2119, Sep. 2013.
6. Y. Chen and W. Tzeng, "Efficient and provably-secure group key management scheme using key derivation," in Proc. IEEE 11th Int. Conf. TrustCom, 2012, pp. 295–302.
7. Y. Chen, J. D. Tygar, and W. Tzeng, "Secure group key management using uni-directional proxy re-encryption schemes," in Proc. IEEE INFOCOM, pp. 1952–1960.
8. S. Goldwasser, S. Micali, C. Rckoff, "The Knowledge Complexity of Interactive Proof Systems", SIAM Journal of Computing, vol. 18, pp. 186-208, 1989.
9. "GoldreichMicali and WigdersonProofs that Yield Nothing But their Validity or All Languages in NP have Zero-Knowledge Proof", JACM, July 1991.
10. Mazhar Ali, Athanasios and Revathi.Dhamotharan "SeDaSC:Secure data sharing in clouds", IEEE Systems,pp:1-10, 2015.