IMPROVE PRIVATE CLOUD DATA SECURITY WITH RBAC-ENCRYPTED SCHEMES

[1]P.M.Suresh, [2]R.Anbarasu,[3]S.T.Saravanan,[4] T.Manigandan

[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor, [4]Assistant Professor,

[1]Department of CSE, P.T Lee Engineering college, Kanchipuram, India,

[2]Assistant Professor, Department of CSE, P.T Lee Engineering college, Kanchipuram, India,

[3]Assistant Professor,Department of CSE, Paavai Engineering College, Salem, India,

[4]Assistant Professor, Department of CSE, SRS College Of Engineering and Technology, Salem, India.

Abstract: The term "cloud computing" refers to a group of computer concepts that involve several machines connected via a real-time communication network, such the Internet. Because it can lower computing costs, cloud computing is an emerging paradigm that is now the focus of much research. The quick development of cloud computing technology has led to an extremely notable rise in the number of cloud services offered. Data security is a difficult problem in the modern world.A collection of computer concepts known as "cloud computing" are those that include multiple devices connected by a real-time communication network, such the Internet. Cloud computing, an emerging paradigm that potentially reduce computer expenses, is now the subject of a lot of research. The number of cloud services available has significantly increased as a result of the technology for cloud computing developing so quickly. Nowadays, data security is a challenging issue.

Keywords: RSA, Digital Signature, Cloud Computing, Internet, Role Back Access Control, and Blowfish Algorithm.

I. INTRODUCTION

The long-dreamed-of idea of computing as a utility—where users can store their data remotely in the cloud and access high-quality on-demand apps and services from a common pool of reconfigurable computing resources—is known as cloud computing. A new business model called "cloud computing" is based on cutting-edge technologies like "server virtualization," which use multi-tenancy and economies of scale to lower the cost of employing IT resources. It also exposes the outsourced data to fresh, difficult security risks. Cloud service providers (CSPs) are independent administrative organizations, therefore outsourcing data essentially means giving up final say over what happens to the owner's data. The usage of a cloud image to symbolize the Internet or any extensive networked system is likely where the name "cloud computing" originated, at least in part. In reality, cloud computing is just using services and resources to carry out tasks with constantly shifting requirements. The cloud is accessed by application or service developers instead of a designated resource or endpoint. The cloud is made up of one or more frameworks that are layered on top of various infrastructures to manage them across many organizations and connect them. Platforms for cloud computing are expanding rapidly. Hardware for clouds can be supplied by businesses themselves (internal clouds) or externally by other parties (hosted clouds). A cloud may be accessible to the world via the internet, limited to a single company or group (private clouds), or be shared by several organizations or groups (hybrid clouds) or the Internet (public clouds) [1].

I. DATA SECURITY ISSUES IN THE CLOUD

Security was the main concern with cloud computing a few years ago. Concerns related to cloud security, including data security, application security, access security, transmission security, storage security, and physical security. The user of cloud computing must guarantee the security of their infrastructure [2]. Data in cloud systems is kept on servers run by cloud providers at a remote location. The cloud provider ought to have safeguards in place to guaranteethat customer data is not directly shriveled.Physical security is no longer within your control when using the cloud approach. You are sharing computer resources with other businesses when you use a public cloud. The very fact that you share a cloud environment could make your data more susceptible to seizures. Should you choose to switch from one cloud provider to another, the storage services offered by each might not be compatible. The guaranteeof consistency and accuracy in data is known as dataintegritymaking sure that the data only modifies in response to approved transactions is the true definition of ensuring data integrity. Two of the more contentious difficulties with cloud computing may have to do with data security and storage, as well as service providers' use of the cloud being observed. Generally speaking, these problems are related to the implementation of cloud services being delayed. For instance, by keeping the data on file within the company while enabling cloud access for it. In the event that bad actors are able to access or delete the offered cloud storage,

personal data is exposed, potentially causing significant harm to each specific user. When it comes to cloud computing, the provider must make sure that their infrastructure is safe and that the data and applications of their clients are safeguarded, and the customer must make sure that the provider has implemented the necessary security measures to protect their data.

III. PROPOSED WORK

Our goal with this proposed work is to secure our cloud data. Since security is the main problem that every user has to deal with. Think of a company where a large number of workers, or employees, are employed. Every user has a unique LOG IN ID and password to keep their data, and ADMIN is in charge of running the entire business. Because there are several restrictions on who can download cloud files, RBAC Administrators can assist prevent unauthorized access to the system. Due to downloading restrictions, any unauthorized user may alter certain files,but the remaining files will be saved. RBAC contributes to cloud data security.

Second, Blowfish facilitates encryption every file will have a public key generated along with a private key that aids in creating the digital signature needed to speed up downloads. The user will have access to this digital signature through mail. In addition, it offers superior security and storage compared to cloud architecture

A sort of (RSA and Blowfish Algorithm combined) would make it more difficult to hack. These algorithms aid in supplying security. Here, we show Figure 1, which depicts the fundamental layout of the task we have in mind.

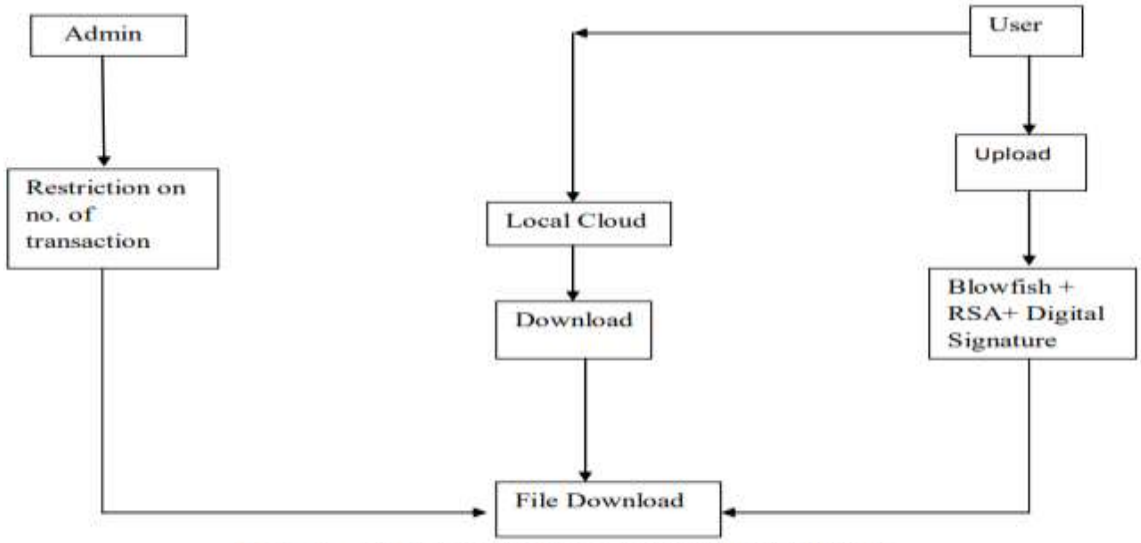

Figure 1 :- Represents the basic design of proposed work

Admin: In an organization, the admin assigns users to roles and determines how many transactions each user can complete in accordance with their role.

User: The ability to upload and download files. Blowfish and RSA schemes are used to encrypt data when a file is uploaded, and a signature is included to lock that data. In the opposite case, when a file is downloaded, Blowfish and RSA methods are used to decrypt data, and a signature is used to unlock the file.

Local Cloud: Data is secured and stored on the Local Cloud. We will go over RBAC, RSA, Blowfish Algorithm, and digital signatures below.

A . Role- Based Access Control

A wonderful technological advancement in the area of access control is ROLE-BASED ACCESS CONTROL (RBAC). Within an organization, a role denotes a particular function and can be viewed as a collection of tasks or obligations related to this role. Administrators define roles based on job skill, authority, and responsibility inside the company. [3].Instead of being issued to users by the administrator, all grant authorizations in an RBAC model deal with roles. RBAC makes sure that only authorized users have access to particular data or resources. Within the organization, roles are determined by the Administrator based on job skill, authority, and responsibility.

B. Blowfish Algorithm

A symmetric block cipher algorithm is called Blowfish. The same secret key is used for message encryption and decryption. Blowing fish has a 64-bit block size; every message that isn't a multiple of 64 bits needs to be padded. It employs a key that can range in length from 32 to 448 bits.fragments. [4].Applications where the key is not changed regularly should use it. It performs noticeably quicker in 32-bit microprocessors with large data caches than the majority of encryption techniques. Figure 3 illustrates how a 16-round Feistel network is used for data encryption.

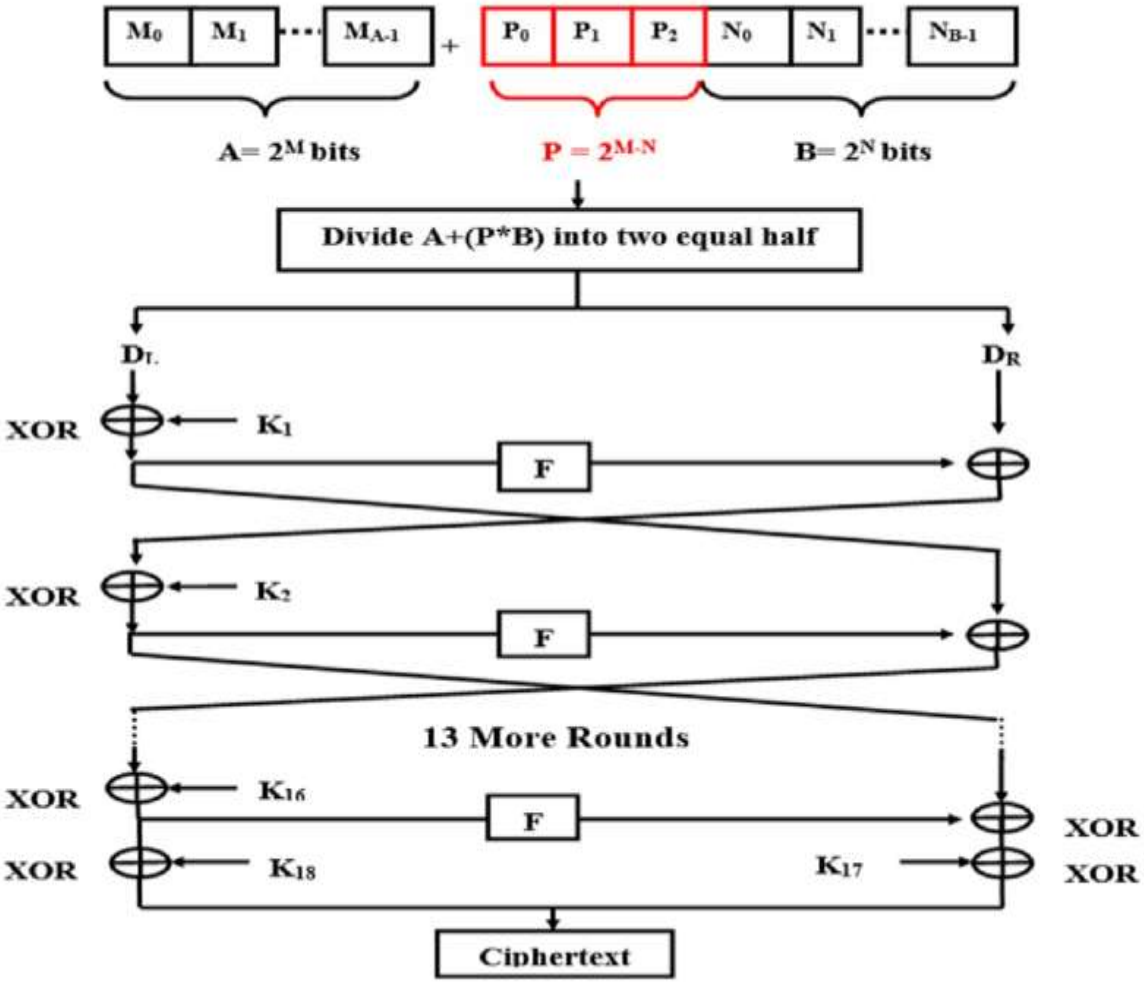

Figure 2. Encryption with Blowfish

C. RSA

RSA stands for Ron Rivest, Adi Shamir, and Len Adleman; they first publicly described the public-key algorithm in 1977. In our proposed work, we use the RSA algorithm to encrypt the data to provide security, ensuring that only the relevant user can access it [5]. Here, we explain the RSA algorithm. It consists of three steps:

1.First-rate Generating , 2. The use of encryption ,3. Encryption

In the cryptography security system, an RSA algorithm is a genetic algorithm[6]. Prior to using RSA methods, we select the two integer values.

Assume that the integer values are P and Q. The value of N is then determined.

N is equal to P × Q. (3.1)

(P - 1) × (Q - 1) = Ø(N) … (3.2)

Next, we select e's value, which is not a factor of Ø(N).

Furthermore, the value of d is determined, and it is connected to the expectation value (e).

ed = 1 mod (N)... (3.3)

Or d = 1 e mod Ø(N)... (3.4)

That is, d = $e-1$ mod Ø(N) (3.5)

According to the Euclidian theorem, d's value is dependent on |Ø(N)|.

The modulus values of d are 1, 2,...n. d = |Ø(N)| + 1 … (3.6)

Both the encryption and decoding processes employ RSA methods.

Key for encryption = (e, N).

Key for decryption = (d, N).

In the event if the message M, then M

E = Me mod N is the encryption. (3.7)

Decode => M is equal to Edmod N. (3.8)

The methods used in equations (3.1), (3.2), and (3.6)

D. Digital Signatures

A digital signature is a mathematical system used to prove that a digital message or document is authentic. Financial transactions, software distribution, and other situations where it's critical to identify fraud or tampering frequently employ digital signatures. An algorithm for creating keys that consistently and randomly chooses a private key from a range of potential keys that are private. The public key that corresponds to the private key is produced by the algorithm. Additionally, some non-repudiation schemes offer a time stamp for the digital signature, ensuring that even in the event that the private key is revealed, the signature is still valid. Digital signatures can also provide non-repudiation, which means that the signer cannot successfully claim they did not sign a message while also claiming their private key remains secret. Anything that can be represented as a bit string can be digitally signed, such as contracts, emails, and messages delivered over other encryption protocols.

IV. IMPLEMENTATION AND RESULT

1. ASP.NET is used to implement the described work. First, we display the snapshot in which the administrator limits each user's download limit. This snapshot shows the list of workers for the company as well as the download limit that the administrator has set. Figure 3 shows the authorization granted. With the aid of RBAC, this restriction offers security. Because without administrator approval, an unauthorized user cannot download the contents.

Fig. 3: Representation for permission taken

2. Figure 4 shows the uploading page where employees can upload files and have them processed. When an employee uploads a file, the file is first encrypted using the Blowfish algorithm. With the assistance of Blowfish, the cipher text is produced. Subsequently, RSA is implemented on it. Additionally, each file generated by RSA has a public and private key. Each file displays

the public key, which is used to create a new session and private key using a digital signature. Algorithm creates a digital signature that is sent to the employee's email.

Figure4. Represents the uploading procedure

The downloading process wherein the employee wishes to download the file is depicted in Figure 5. However, in order to download a file, you must have a digital signature, which you can get via the employee's email. And a public key is visible on their right side.

Figure 5. Represents the downloading procedure

4. The Signature key, which is needed to download the files, is shown in Snapshot Figure 6.The user must provide a signature in order to download a file. Additionally, the user can access the Signature via mai

Figure 6. Represents the Signature key

Figure 7 illustrates the process of downloading a file within a signature. An employee accessed the file after entering their signature. A file containing a signature is downloaded when an employee enters. In a similar manner, a second file is downloaded using Signature.

Figure7. Downloading a file within Signature.

3. The downloading of a page within the No Permission To Download Message is depicted in Figure 8. Just two files have been downloaded because an employee has restricted access. due to an administrator's restrictions on Employee. When an employee wants to download a third file after seeing the first two, a notification notifying the administrator is generated.

Figure 8. Represents the downloading files within Restriction

6. To transform an image into an encrypted form of data, Blowfish and RSA are used in the encryption process. Figure 9 below illustrates the encryption process using the RSA and Blowfish algorithms.

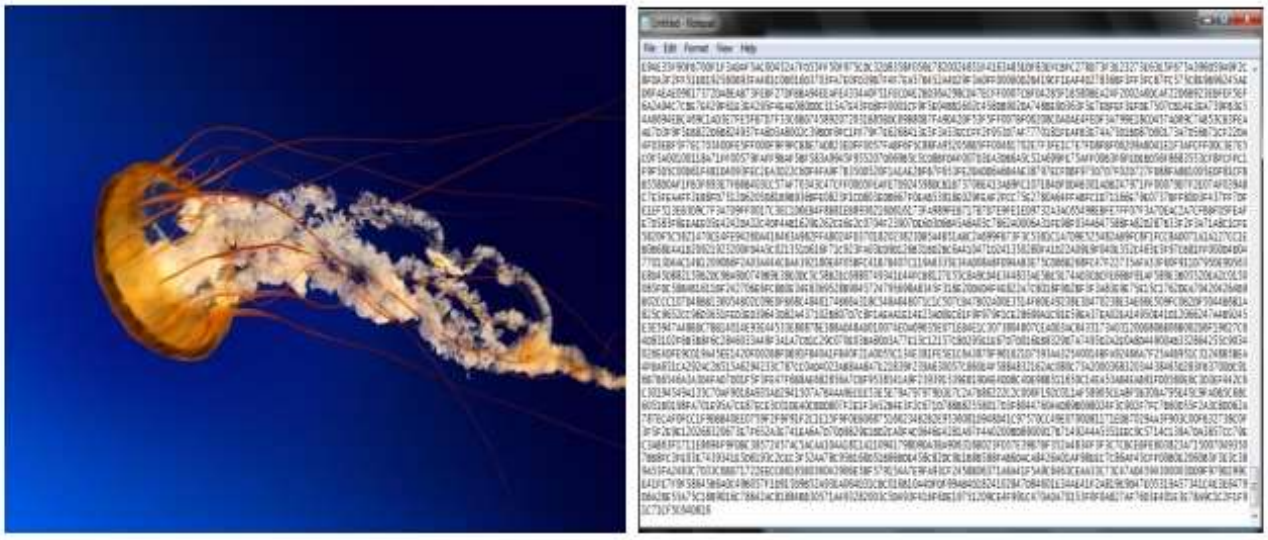

Fig.9. Encryption by using Blowfish Algorithm and RSA

V. CONCLUSION AND FUTURE AREA

The concept of cloud computing, which views computers as an on-demand service, is still relatively new and still developing. The organization forfeits control over the data if it decides to migrate to the cloud. Cloud security is based on encryption and trusted computing. As a result, only the authorized user has access to the data in our proposed task. Due to encryption mechanisms, even if an unauthorized user (intruder) catches the data and obtains it accidently or on purpose, he will be unable to decrypt and read it. We will prevent illegal access to the system with the use of RBAC. The kind that uses RSA and Blowfish Algorithm together would make it more difficult to hack. Additionally, it offers an improved method for storage and security.My suggested work will be very helpful in the future to improve cloud computing security. Reliable authentication systems are necessary as the requirement for security grows because they can reduce illegal access and help to protect data.

REFERENCES

[1]. Uma Somani, “Implementing Digital Signature with RSAEncryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010). Volume 64,pp.211-216.

[2]. Leena Khanna “ Cloud Computing: Security Issues And DescriptionOf Encryption Based Algorithms To Overcome Them”International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3 March - 2013, pp. 279-283.

[3]. Wei-Tek Tsai “Role-Based Access-Control Using ReferenceOntology in Clouds”978-0-7695-4349-9/11 $26.00 © 2011 IEEEDOI 10.1109/ISADS.2011.21.

[4].Ajit Singh, “Securing Data by UsingCryptographywithSteganography”“International Journal ofAdvanced Research in Computer Science and SoftwareEngineering “Volume 3, Issue 5, May 2013 ,pp.404-402.

[5].RashmiNigoti "A Survey of Cryptographic Algorithms for CloudComputing" IJETCAS 13-123; March-May 2013, pp.141-146.

[6]. ParsiKalpana "Data Security in Cloud Computing using RSAAlgorithm" International Journal of Research in Computer andCommunication technology, IJRCCT, ISSN 2278-5841, Vol 1,Issue 4, September 2012.

[7]. Esh Narayan" To Enhance the data security of cloud in cloudcomputing using RSA Algorithm", Bookman International Journalof Software Engineering, Vol. 1 No. 1 Sep. 2012 ,ISSN No. 2319-4278.

[8] Pradeep Bhosale" Enhancing Data Security in Cloud ComputingUsing 3D Framework & Digital Signature with Encryption",International Journal of Engineering Research & Technology(IJERT) Vol. 1 Issue 8, October – 2012 ,ISSN: 2278-0181.

[9]. VishakhaLokhande" Efficient Encryption and Decryption Servicesfor Cloud Computing", International Journal of SocietalApplications of Computer Science,Vol 1 Issue 2 December 2012ISSN 2319 – 8443.

[10]. RuWei Huang, Si Yu, Wei Zhuang and XiaoLinGui, "Design ofPrivacy-Preserving Cloud Storage Framework" 2010 NinthInternational Conference on Grid and Cloud Computing.

[11]. FarzadSabahi, "Cloud Computing Security Threats andResponses," IEEE Trans. on Cloud Computing., vol. 11, no. 6, pp.670 { 684, 2002.}.

[12]. Mohammed Achemlal, Sa¨ıdGharout and ChrystelGaber "TrustedPlatform Module as an Enabler for Security in Cloud Computing"Vol 978-1-4577-0737-7/11/$26.00 ©2011 IEEE.

[13]. Jianfeng Yang, Zhibin Chen "Cloud Computing Research andSecurity Issues" Vol 978-1-4244-5392-4/10/$26.00 ©2010 IEEE.

[14]. Victor Echeverr´ıa, Lorie M. Liebrock, and Dongwan Shin"Permission Management System: Permission as a Service in CloudComputing" 2010 34th Annual IEEE Computer Software andApplications Conference Workshop.