WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Achieving New Technique in Cloud Computing Security Data Using Blowfish Algorithm

R. Sakthi Devi [1], S. Ramya [2], R. Suganya [3], G. Suguna [4], Dr .P. Senthil Pandian[5]

[1,2,3,4]Assistant Professor, Department of Computer Science and Applications, Farouk Educational Trust, Perambai, Villupuram District, Tamilnadu – 605110, India.

[5]Associate Professor, Maduari, Tamil Nadu, India.

ABSTRACT

Due to its potential to lower processing costs, cloud computing is an emerging paradigm that has quickly become one of the hottest areas of research in the field. The most intriguing and alluring technology today is the ability to deliver services to customers on demand over the Internet. Distributed data and resources are kept in a public environment using cloud computing. Although cloud computing is effective and promising, data security is difficult because users are far from the data. Consumers may be interested in this technology for a variety of reasons, including storage limitations, dependability, scalability, and accessibility to real-time information.

As a result, it is undoubtedly growing and becoming organized in daily life. Security in cloud computing has always been crucial to the level of quality of service offered by cloud service providers. Today, cloud computing is an emerging technology that is also a technical and social reality. The main barrier to the adoption of cloud settings is security. We suggest a way to secure data storage in the cloud utilizing public key cryptography and the RSA algorithm to ensure data security. The security services that are discussed also cover key creation, encryption, and decryption in virtual environments.

Keywords: Cloud Computing, Cloud security, Data Security, Blowfish Algorithm, RSA Algorithm.

I. INTRODUCTION

A common pool of reconfigurable computing resources (such networks, servers, storage, applications, and services) networked on demand over the Internet is what is referred to as cloud computing. Cloud computing is the literal definition of employing remote servers to process or store data. These servers are typically accessed through the Internet. often reachable via a web browser. One illustration is the online storage of files on servers.

Data security is always crucial, and cloud computing's critical nature and the vast quantities of complex data it stores make this need much more pressing. Future impediments to a larger adoption of cloud computing services look to be privacy and data security worries. There are several data changes and difficulties to overcome as many businesses move their data to the cloud. Application of suitable data security procedures and countermeasures is only one aspect of efficient cloud data security. Authentication and authorization of users are the mainstays of computer security procedures..

Every cloud service requester, whether an individual or a business, should ask the right questions of the cloud provider before hosting their data or applications on the cloud. Potential cloud providers should let you know: are they financially sound? Do they have good security policies and procedures in place? If the infrastructure is used to host shared data with many other users or is it separated by virtualization. Each message block is mapped to an integer value.

The RSA algorithm consists of a public key and a private key. User data is first encrypted and then stored in the cloud. If necessary, the user makes a data request to the cloud provider; the cloud provider authenticates the user and provides the data. RSA is a block cipher where each message is an integer. RSA consists of public and private keys.

In our cloud environment, the public key is well known, while the private key is known only to the user who originally owned the data. Therefore, the encryption is done by the cloud service provider and the decryption is done by the cloud user or consumer. Once the data is encrypted with a public key, it can only be decrypted with the corresponding private key.

II. SERVICES IN CLOUD COMPUTING

Different types of services are defined by the three layers shown below.

i) Infrastructure as a Service (IaaS): This layer is the lowest layer and provides infrastructure support services.

ii) Platform as a Service (PaaS): This is a middle layer that provides platform-based services and provides an environment for convenient client applications.

iii) Software as a Service (SaaS): This tier is the top tier and includes all applications offered as on-demand services.

In cloud environments, security protocols must meet the following requirements.

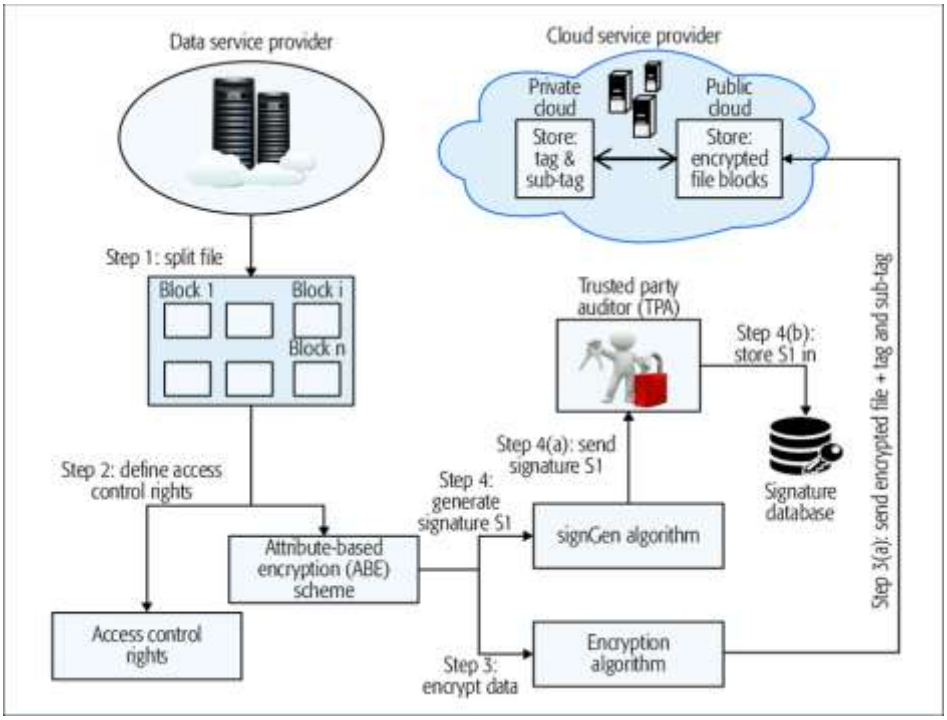
Authentication: It confirms the identity of a person. The credentials provided will be compared with the database. If the credentials match then the user is granted is granted authorization for access.

Data anonymity: It is the process of encrypting the data, so that it cannot be accessed by unauthorized user.

Access control: The users access desires should not be known to any unknown entity.

Forward security: If the password or secret key is compromised, the past sessions must still be protected.

Architecture The architecture of secure data storing and resource allocation in Cloud Computing is shown in Figure 1. Different user's first register in the cloud. Security provider checks the authentication of the user to upload a file of the owner by generating a private key. The encrypted file is stored in the cloud server. Worldwide end clients access the file with permission of the respective file owner. Any file requested from the authorized user is checked by the availability of the resource in the cloud storage. The resources availability is stored in a separate file, i.e., called reliability check. The virtual machine allocates the resources or resources are not allocated. If the file is present, the end user easily receives the file or else if the file is corrupt then the file is regenerate and delivered to the end user based on demand. Security is provided by encrypting the private key in constant size.



III. WORKING OF RSA ALGORITHM AND BLOWFISH ALGORITHM

RSA algorithm

It uses the following procedure to produce public and private keys:

Select two large prime numbers, p and q.

1. Multiply those numbers to find n = p x q, where n is known as the modulus for encryption and decryption.
2. Choose a number e less than n, in order to make n is relatively prime to (p - 1) x (q -1). It means that e and (p - 1) x (q - 1) have no common factor except 1. Choose "e" such that 1<e < φ (n), e is prime to φ (n) gcd (e,d(n)) =1
3. If n = p x q, then the public key is <e, n>. A plaintext message m is encrypted using the public key <e, n>. To generate cipher text from the plain text use the formula given below

C = me mod n

4. To determine the private key, we use the following formula to calculate the d such that:

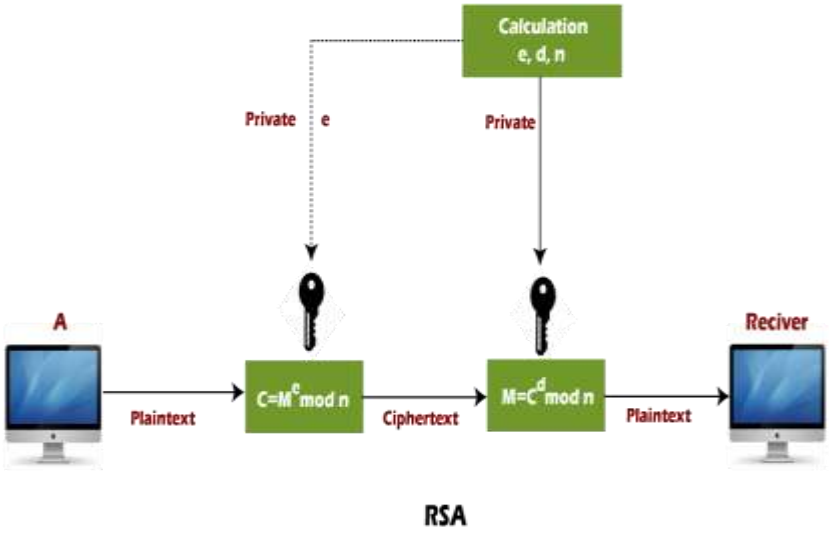
   De mod {(p - 1) x (q - 1)} = 1

Or

De mod φ (n) = 1

5. The private key is <d, n>. A cipher text message c is decrypted using private key <d, n>. To calculate plain text m from the cipher text use the following formula given below

   m = cd mod n



RSA

The above image depicts how encryption and decryption done using RSA Algorithm

Blowfish Algorithm

Blowfish has a block size of 64 bits and uses variable length keys, from 32 bits to 448 bits. It consists of 16 Feistel-like iterations, where each iteration operates on 64-bit blocks divided into two 32-bit words. Blowfish uses a single encryption key to encrypt and decrypt data. The blowfish algorithm consists of two parts :

1.Data encryption. Data encryption takes place via a Feistel network of 16 rounds, with each round consisting of a key-dependent permutation and a key- and data-dependent substitution. Large key-dependent S-boxes work with fallback methods and are an integral part of Blowfish's data encryption system. All encryption operations are XOR (a type of logic gate) and addition of 32-bit words.

2. Key extensions and sub keys. During key expansion, a key with a maximum size of 448 bits is converted into several arrays of sub keys totaling 4168 bytes. Sub keys are an integral part of the Blowfish algorithm, which uses a large number of sub keys. These sub keys are pre computed before encryption or decryption.

In Blowfish, the P array consists of 18 32-bit sub keys and four 32-bit S-boxes with 256 entries each. The sub key is calculated as follows:

1. Array P and box S are initialized with a fixed string of hexadecimal digits for pi.

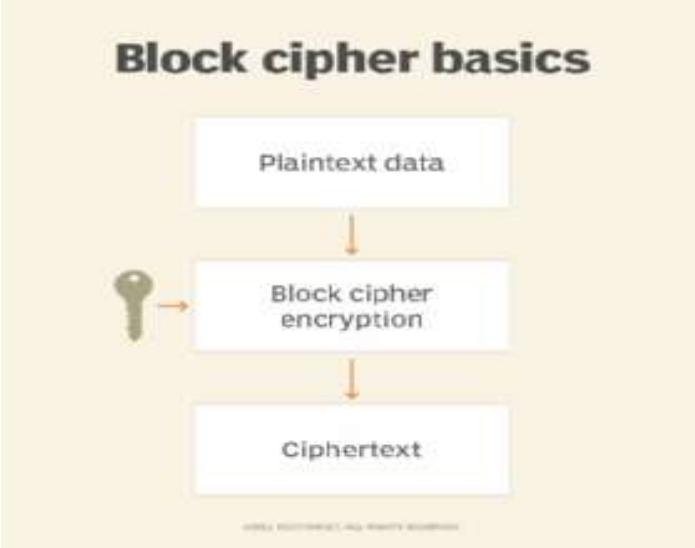
2. The first element of array P (P1) is now XOR ed with the first 32 bits of the key, P2 is XOR ed with the second 32 bits, and so on until all elements of array P are XORed with Key is XORed to pieces.

This output is encrypted by Blowfish using the modified sub key.

6. The output of step 5 modifies P3 and P4 in the P array.

7. This process continues until all P arrays and four S boxes have been modified.

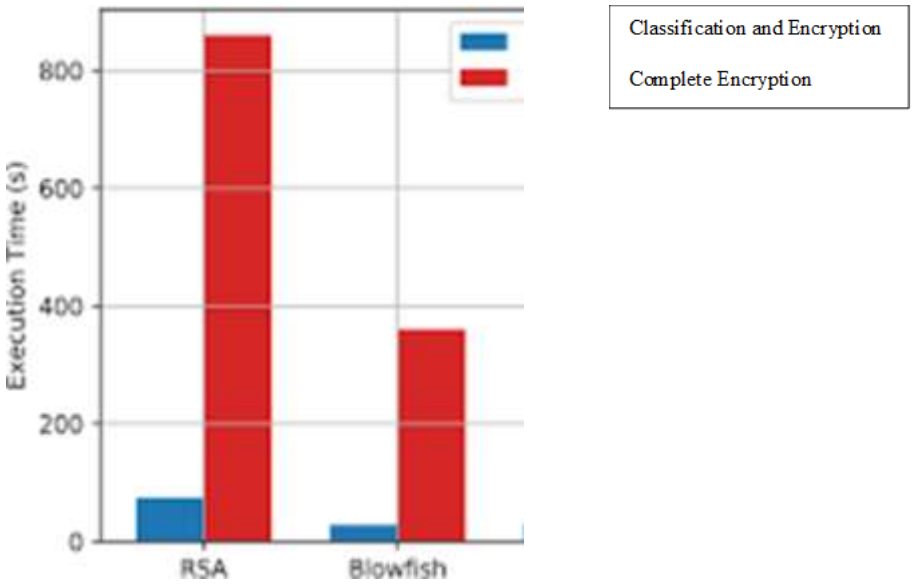
Blowfish was run a total of 521 times to spawn all children and processes, or approximately 4 kilobytes (KB) of data.



IV. HOW TO SECURE DATA IN CLOUD STORAGE

In the field of cloud computing, the cloud provider will in most cases be the data processor, passive processing the data, such as storing the data on its platform. Depending on the type of cloud used, the Cloud provider responsibilities may 4044 include provision of infrastructure, physical 4044 premises security, operating system, and network security. On the other hand, the cloud client will become the data controller, actively processing the data for its own business purposes. Depending on the service model used, its responsibilities may include control of the virtual infrastructure and any application security. In order to protect the data against various attacks and the integrity of data encryption, data encryption must be performed before transmission or storage. Governments, military, financial institutions, hospitals, and private companies process confidential images of their patients (in hospitals), geographic areas (in search), enemy positions (in defense), products, financial status. Much of this information is now collected and stored in the electronic computer and transmitted to other computers via the network. Should this data fall into the wrong hands of, this security flaw could cause to reject the war, abuse, etc. 4044 Protecting confidential images is an ethical and legal 4044 requirement. Cryptography is a method of storing and transmitting data in a format that only designated people can read and process. It's a science of protecting information by encoding it in an unreadable format. It is an effective method of protecting sensitive information when stored on media or transmitted over network communication channels. The best solution to deal with security issues is data encryption. Various algorithms exist to encrypt data in cloud computing such as DES, 3DES, Blowfish, AES, etc.

V. COMPARISON CHART FOR RSA AND BLOWFISH ALGORITHMS



VI. CONCLUSION

The concept of cloud computing, which is still developing, views computing as an on-demand service. The moment a company decides to migrate its data to the cloud, it forfeits control over that data. As a result, the value of the data directly affects the level of protection required to keep it secure. Cryptography and trustworthy computing are essential for cloud security. As a result, only the authorized user can access the data in our proposed task. Even if an intruder (unauthorized user) takes the data, whether unintentionally or on purpose, he is unable to decrypt it and retrieve the original data. Therefore, RSA algorithm implementation provides data security.

VII. REFERENCES

[1]. P.Kalpana, "Cloud Computing – Wave of the Future", International Journal of Electronics Communication and Computer Engineering, Vol 3, Issue 3, ISSN 2249–071X, June 2012.

[2]. Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 , 1836-1840, 2011.

[3]. Zaigham Mahmood, "Data Location and Security Issues in Cloud Computing", Proceedings of International Conference on Emerging Intelligent Data and Web Technologies-2011.

[4] Vishwa gupta, Gajendra Singh, Ravindra Gupta, "Advance Cryptography algorithm for improving data security", International Journal of Advanced Research in Computer

[5]. G. Jai Arul Jose, C.Sanjeev, Dr. C.Suyambulingom, "Implementation of Data Security in Cloud Computing", International Journal of P2P Network Trends and Technology, Vol 1, Issue 1, 2011. [9].William Stallings, "Network Security Essentials Applications and Standards", Third Edition, Pearson Education, 2007.

[6] Gutte, P., Wankhade, J.V. and Mote, S., 2020, Key Generation & Access Control Policy in Cloud Data Sharing, (No. 2562). EasyChair.

[7] Hidayat, T. and Mahardiko, R., 2020. A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing. International Journal of Artificial Intelligence Research.

[8] Dr.P.Senthil Pandian, V.Vivek,and S. DuraiPandi "An Analysis for Embedded IoT Devices in Device-to-Device Communications" Journal of Advanced Research in Dynamical and Control Systems, Vol. 10,02-Special Issue, pp.1220-1224,2018

[9] Kumar, Y.K. and Shafi, R.M., 2020,An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem, International Journal of Electrical and Computer Engineering, 10(1), p.530.