Cloud data security and various security algorithms

Kanika Tyagi\textsuperscript{1}, S.K Yadav\textsuperscript{2}, Mayank Singh\textsuperscript{3}

\textsuperscript{1}Noida International University, Greater Noida, U.P,India
\textsuperscript{2}Noida International University, Greater Noida, U.P,India
\textsuperscript{3}Consillio Intelligence Reserach Lab, Noida, U.P,India

Email: kanikat374@gmail.com

Abstract. The term Cloud computing is a most trending and promising technology. It is the most basic need for many organizations. Cloud technology has many advantages as user can access the files from anywhere over the internet. It has also a very known feature of using the resources according to their demand and user does need to pay extra charges for the unused resources. In Cloud Computing user do not need to carry all their documents with them as cloud access is global. But as Cloud computing means sending data over internet so sometimes there may be security issues and threat of intruder attack at the time of data transmission. As traditional banking industry is totally changed and now the total control in the hand of customer rather than the bank. In banking industry cloud computing provides various features viz; cost saving, business continuity, business agility and time saving. but as data in bank is the most crucial data so cloud security is the first priority for every bank before adopting cloud. Security at cloud is the biggest obstacle for the banking industry to adopt this trending technology and its services. So there is need to provide security to the cloud. This paper aims on cloud basic methodology and analyze some security algorithms and their applicability in cloud banking environment

Keywords: cloud computing, RSA, Twofish

1. Introduction

With the advancement in technology, infrastructure in IT is also getting advance day by day. Earlier organizations used Relational databases to store their data which was not cost effective way for storage of data. After that, concept of grid computing and cluster computing came into existence. It enables to share data in clusters which was geographically dispersed. But today, cloud computing has totally change the idea of storage. Somewhere it is basically derived from the concept of cluster computing and grid computing but it has some add on features.

Although cloud system provide the organizations global and fast access of data but security of files is the main consideration for the user. There is encryption to secure the transmission. The data is said to be secure if it has integrity, authenticity and confidentiality. This paper focuses on to maintain these aspects of security by the blend of RSA, SHA and twofish algorithm.
According to NIST, “It is a model having common pool of shared resources that can be accessed with very feweffort or without interacting service provider. It has five basic characteristics, four deployment models and three service models [1]. It’s a buzz in today’s world which has totally changed the way to access the data.

![NIST Cloud Computing Structure](image)

1.1. Cloud deployment models

There are four types of deployment models:

- Public Cloud
  
  In this, information is accessible to the different organisations from anywhere. This type of cloud is overseen by a third party who rent out the resources to the end client [2] and user need to pay only as the usage of resources. In public cloud as different organizations share information across the network so there are frequent chances of intruder’s attacks and data tempering. Example: Amazon, AWS, Microsoft etc.[3]

- Private cloud
  
  This type of clouds is accessed only by the authorized users. This type of cloud is basically for the particular organization and only that organization can share the application over the cloud. As private cloud has limited and authorized access so it provides higher security, privacy and more control. But it is good for access when there is small number of user who accesses the information. Example: Intranet. [4]

- Hybrid cloud
  
  It is the most adaptable model having a mix of public and private cloud. Thus it provides the features of various deployment models in terms of security and cost. Main features of hybrid cloud are scalability, security and flexibility.[3]
• Community cloud

Community cloud is shared between different organizations under some terms and conditions who get ready to share the same resources for some purpose. So community cloud is a extended form of public cloud with more secured features. This type of cloud can be deployed within the same organization or different organization.[3]

1.2. Cloud computing service models

• Infrastructure as a Service (Iaas)

It provides direct access to all software and hardware resources. In this model owner of the cloud provides the various cloud facilities like processor, networking resources, servers and other software facilities. This is the controlling layer of various operators. In IaaS, enterprise rent out their infrastructure to external environment and customer pays as per the usage of resources. Example: Flexiscale, AWS: EC2 etc. [4]

• Platform as a Service (PaaS)

It is a supplier model which supplies the stage admittance to the clients so they can run their own applications and customized software on the cloud. Client is free about keeping up with capacity; hard drives and workers. It additionally have some inherent devices with some predefined capacities which assists the client with conveying the application according to the interest. In any case, primary issue with this is that the conveyed applications are rely upon climate and can't run on any different vendor's environment. Example: Google App Engine, Microsoft Azure etc.[5]

• Software as a Service(SaaS)

As the name implies it serves software to users as cloud service. This process is done through web browsers. In this user does not need to have license. Users can adjust the cost for the software development, maintenance and operation Example: DropBox, Google and Ms Office Web. [6]

1.3. Cloud Computing Characteristics

• Service as per demand

Cloud is a pool of information from where various cloud services like email; network server etc. can be accessed without any contact with service provider. [1]

• Broad network access

As data in cloud is geographically stored over the network. It has millions of server and data from these servers can be accessed by standard mechanism and from laptop, mobile phones etc. [9]

• Resource Pooling

The resources of provider are grouped together to fulfill the needs of various consumers. Resources are assigned and reassigned to the consumer on the basis of their demand. The pooling of resources like memory, network bandwidth maintains the economy.

• Measured Services

Resources usage on cloud computing is transparent to both the parties, i.e cloud service provider and client. As in daily life electricity is charged as per the usage, similarly the resources on the network. More usage leads to more payment. For example various telephone providers sell their plans for voice and data services and data management services to the various users on contractual basis.
• Multi-Tenant Model
  Cloud follows a multi-tenant model. One single application or software serves many clients, and each client is called a tenant. Tenants share a common access with some specific privileges to the software instance. [9]

1.4. Cloud Security Issues

Although the cloud environment has proved itself to be a milestone in the field of IT and also provides many features like flexibility, reliability, unlimited storage and fast processing, but security is still a greatest obstruction for organizations to adopt it. Some security issues are as follows:

• Trust
  Trust is basically a foundation of transmission. Trust management should exist between cloud service provider and user. User must have a surety that service is reliable and whether their data is free from all malicious attacks. This service is done by Service Level Agreement (SLA), act as a document between the Cloud Service Provider and user which comprises all the duties of service provider. [7]

• Confidentiality
  It means to maintain the secrecy of important information. On cloud all the information is globally stored at different locations, it becomes a sensitive issue. As the number of users increase on the cloud this problem also increases. [7]

• Integrity
  Integrity states that transmitted to be free from alterations across the network but as on the cloud there are trapdoors for intruders so maintain integrity is a huge task. [8]

• Availability
  It says that the demanded data, hardware and software must be available to the user. But as on cloud data is globally dispersed which causes intruder attacks and results to unavailability of data sometimes. [8]

2. LITERATURE SURVEY

Sanjoli and Jasmeet [10] stated that cloud security can be achieved by using a blend of two algorithms EAP-CHAD and Rijndael Encryption algorithm. The main aim of Rijndael algorithm is to provide encryption and EAP-CHAP for authenticity. This process comprises of four steps. In the first step request formulation is from user to service provider is done. Then, at that point in the wake of checking the approval using EAP-CHAP an affirmation send back to the client and client encode the information using Rijndael algorithm and transfer the information to the server. When the encoded information put away on the server, it tends to be unscrambled utilizing a similar key which utilized in encryption. Subsequently customer side security was considered there.

Jasleen Kaur, Sushil Garg [2] implemented a mixture of RSA and blowfish algorithm. RSA is used for validation and verification purpose while blowfish is used for encryption. The algorithm is implemented in Java Netbeans. It was concluded that this blend takes few fraction of time to encrypt and decrypt the data and its encryption is also not easily understandable. One algorithm was public key cryptography and other is secret key cryptography.
Somani, Uma, Kanika Lakhani and Manish Mundra[6], stated various characteristics of cloud and mention the process to generate digital signature using RSA algorithm. It comprises of 5 steps. This process comprises of key generation, digital signature, encryption, decryption and signature verification. With this there was a bright future of cloud security.

Garima Saini and Naveen Sharma [11] stated that cloud has many servers and it is based on client-server architecture. So to protect the cloud new security mechanism was implemented. It comprises the blend of two algorithms i.e. Digital Signature Algorithm and Data Encryption Standard with steganography to enhance the security. By this authenticity, security and data integrity is maintained. But it was observed that its time complexity was high as the complete mechanism is one by one process.

Neha, Mandeep Kaur[4] represented the AES, blowfish and two-fish algorithm. An architecture was deployed which comprises of four steps. First step is registration module and next is file upload module. There were two options i.e. AES with blowfish and AES with twofish to encrypt the file. After analyzing it is found that twofish gives better result than blowfish as there are no weak keys found in twofish unlike blowfish. Twofish is robust and faster. [4]

To protect data in cloud computing Cunsoslo et al.[12] suggested a technique that comprises blend of symmetric and asymmetric algorithms. However, this strategy permitted simply owner to get to the information which violate the concept of resource sharing in cloud computing.

Hashizume et al. [13] showed various security problems in SaaS, PaaS and IaaS, security models of cloud. This paper also presented identification of major vulnerabilities in cloud computing but it does not presents any technical implementation of suggested solutions.

3. VARIOUS SECURITY ALGORITHMS

RSA: RSA was developed by Rivert, Shamir and Adleman in 1977. It is public key cryptography algorithm. RSA supports authentication and non repudiation of data which ensures that data is coming from a reliable source and there is no duplication. [14] RSA contains two keys: public key and private key. Private key act as a secret key between both the parties and public key is known to everyone. In RSA private key is used for signing the document.

- Take two random large prime numbers u,v.
- Find z=u*v
- Now find φ (z)=(u-1)(v-1)
- Pick e such that e is prime co-prime number of φ(z) such that gcd(e, φ(z))=1
- Find d such that d.e mod φ(z)=1; d=private key exponent

The public key has a modulus z and e. The private key consists d and its value must be kept secret.

Twofish Algorithm

Twofish is an extended form of blowfish algorithm. It is 128 block cipher algorithm that accepts a variable length upto 256 bits. Its cipher is a 16 round feistel network with a bijection function f which comprises of four key dependent 8 by 8 S-boxes, 4 by 4 Maximum Distance Separable Matrix, a Pseudo Hadmard Transform, bitwise rotation and a key schedule.[15]
Given two inputs, $a$ and $b$, the 32-bit PHT is defined as:

$$a' = a + b \mod 2^{32}$$

$$b' = a + 2b \mod 2^{32}$$

The diagram above is a pictorial representation of Twofish. It has a plaintext of 128 bits.

- Plaintext is parted into four 32 bits.
- It comprises 16 rounds.
- In each round, the $g$ function takes two words on the left as input.
- $g$ function contains S-boxes which take 8 bits of input and generate 8 bits of output.
- The results are interpreted as a vector of length 4 and multiplied by a $4 \times 4$ Maximum Separable distance matrix.
- The results are assembled using a Pseudo-Hadamard Transform.
- The two results are Xored.
- The left and right halves are swapped for the next round.
- After that, the swap of the last round is reversed and the four words are xored with four more keywords to produce the ciphertext.
4. ANALYSIS OF ALGORITHMS FOR BANKING CLOUD SECURITY

As cloud computing basically strike the idea of storing and managing data on virtualized servers so that customer and organizations all over the world can access the data from anywhere at anytime. So there should be some strong secure mechanism.

RSA algorithm for key generation is not an appropriate choice for banking cloud security as using RSA algorithm for key generation because after generating the key that key must be stored somewhere so there should be key management system. Key management is the most crucial phase to manage in cryptosystem. This key can be accessed or stolen by employees without into consideration of end user. So we must think about technique where key management is not required because any breach in key management can lead to lost of data or theft of data. There are many ways to find the value of modulas \( n \) and the value of \( p \) and \( q \) so this algorithm is not as much secure for banking cloud environment. For this, there should be some mechanism which can help the bank to establish a secure cloud so that the crucial data of customer can be saved.

Twofish algorithm is a block cipher algorithm. But it is weaker than AES algorithm for encryption. If we compare both the algorithms to encrypt the 240KB of data (plaintext). The result is shown below:

| Algorithm          | AES  | TWOFISH |
|--------------------|------|---------|
| Original Text      | 240 KB | 240KB   |
| Cipher Text        | 847KB | 955KB   |
| Speed              | Faster | Fast   |
| Security           | Excellent | Secure |
| Space              | Less than twofish | More than AES |

5. CONCLUSION AND FUTURE SCOPE

Thus it can be concluded that RSA algorithm has some features but it is not a strong mechanism to secure the banking data on cloud. Similarly for encryption also twofish cannot be a best choice because there may be some weaknesses in S-boxes also and it is slower than AES algorithm. So in future we will try to find some other strong mechanism to secure the cloud data as password is the main key component in banking industry so something will be done to generate the most secured key using password based key derivation function.

References

[1] https://csrc.nist.gov/publications/detail/sp/800- ........1.45/final

[2] Jasleen Kaur and Dr, Sushil Garg.”Security in cloud computing using hybrid of algorithms” International Journal of Engineering Research and General Science, volume3,Issue 5, (2015).

[3] Deepika Jalhotra, Dr. pradeep Kumar, Shalini aggarwal.” A review on cloud security and its issues using various symmetric key encryption algorithm”.International Journal Of Advanced Research in Computer Science,Volume:8,2017

[4] Neha, Mandeep Kaur.” Enhanced Security using Hybrid Encryption Algorithm”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 7, July 2016.

[5] Manpreet Kaur, Hardeep Singh.”A review of cloud computing security issues”, International Journal of
Advances in Engineering & Technology, ISSN: 2231-1963, 2015

[6] Somani, Uma, Kanika Lakhani, and Manish Mundra. "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud.

[7] William Stallings, Cryptography and Network Security.

[8] Kartik S, Muruganandam A. “Data Encryption and Decryption by using Triple DES and Performance Analysis of Crypto System”, International Journal of Scientific Engineering and Research, Volume: 2 Issue: 11.

[9] Sonali Madireddi. "Implementing Cloud Security by Encryption using Block Cipher Algorithms", International Journal of Applied Information System, Volume: 4.

[10] Sanjoli, Jasmeet Singh. "Cloud data security using authentication and encryption technique.” Global Journal of Computer Science and Technology 13.3 (2013).

[11] Saini, Garima, and Naveen Sharma. “Triple Security of Data in Cloud Computing,” International Journal of Computer Science & Information Technologies 5.4 (2014).

[12] V. D. Cunsole, S. Distefano, A. Puliafito, and M. Scarpa, “Achieving information security in network computing systems”, Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC’09.), 2009, pp. 71-77.

[13] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing”. Journal of Internet Services and Applications, vol. 4, 2013, pp. 1-13.

[14] William Stallings, “Cryptography and Network security”.

[15] G. Hanumantha Rao, G. Narender, T. Balaji, M. Srilatha. “Security Providing using Blowfish, RSA and SHA-512 Algorithms”, International Journal of Computer Science And Technology.

[16] Aparna, K, Jyothy Solomon, Harini . M, Indhumathi . V, “A Study of Twofish Algorithm”, Volume: 4, Issue 2.