

Security in Cloud Computing using Hybrid of Algorithms

Jasleen Kaur¹, Sushil Garg²

[1]Student,M.tech(CSE),RIMT,Mandi Gobindgarh,Punjab

E-mail: jasudhingra@gmail.com

Contact No.: 9914341118

[2]Principal, ,RIMT,Mandi Gobindgarh,Punjab

Abstract-Cloud Computing is a fast evolving technology in the field of IT industry. It is well known for its on demand service to the users remotely over Internet. It provides the users with the resources as per their demand and also enables the users to pay as per their usage of resources. Also, it helps the users to access the cloud from anywhere over Internet. This is a big advantage of cloud computing since one need not carry all the documents always since cloud access is global. Although the cloud storage is centralized but cloud access can be done remotely. This means that it is possible that there can be security breaches or any intruder attack while fetching or storing the data onto cloud. So, security of cloud is really important. So, this paper introduces a new security approach using hybrid of two algorithms: RSA as Digital Signature and Blowfish Algorithm.

Keywords- cloud computing, security, deployment models, service models, security, RSA as digital signature, Blowfish algorithm

1 Introduction

Cloud Computing is being viewed as an emerging field in the world of IT industry as it provides scalable “on demand service” to the users over Internet. Cloud Computing aims at providing resources to the users as per their demand only. Cloud allows users to pay as per their requirement and need not pay for the not required resources hence saving money. It is a smart way to use or share resources as it provides business to many people remotely and at the same it lets customers get the resources of their choice all at one place over Internet. Thus, buyer and vendor need not come face to face in order to make the deal and both can be served for their purposes remotely over Internet through Cloud Computing. There are a lot of companies that have come up with their own clouds such as Google, Amazon, Microsoft,IBM,Oracle and so on, to help people get the benefits of cloud services. The cloud provides services on three different layers: Software as a Service(SaaS), Platform as a Service(PaaS) and Infrastructure as a Service(IaaS). These layers have been explained below. Also, cloud is of various types such as Private Cloud, Public Cloud, Hybrid Cloud and Community Cloud. These types are discussed further.

1.1 Deployment Models

There are different deployment models in cloud computing. These are:

- a.) Private Cloud: Private Cloud is the one in which cloud infrastructure is established within the organization and provides limited access to the users. Since, only privileged users can access the resources on the cloud, it is considered as most secure of all other deployment models. It is deployed where the number of users accessing the information is small.
- b.) Public Cloud: Public Cloud is the one in which cloud infrastructure is shared among different organizations. The public cloud is managed by some third party who lease out the resources to the organizations as per their demand. Hence, the public cloud supports the feature pay-as-you-go pricing. Public clouds are vulnerable to data tampering as there are multiple organizations accessing the applications on sharing basis and hence, it may give easy access to some intruder.
- c.) Hybrid Cloud: Hybrid Cloud is the combination of different clouds. As it is the combination of models, it offers the advantages of multiple deployment models. It provides ability to maintain the cloud as recovery of data is easy in this cloud. It provides more flexibility.
- d.) Community Cloud: Community Cloud is the one in which the cloud infrastructure is shared between different organizations with same interests or concerns. The organizations having same requirements (like security, policy, etc.) agree to share the resources from the same party or cloud vendor. Hence, community cloud is basically a public cloud with enhanced security and privacy just like that in private cloud. The infrastructure may be maintained within the organization or outside the organization.

1.2 Cloud Computing Service Models

- a.) Infrastructure as a Service (IaaS):

IaaS is the last layer of the cloud computing stack and this layer provides the consumers with various facilities like that of storage, processors, servers, networking and other hardware facilities and as well as some software facilities like virtualization and file system. This layer controls and manages various operations required by the consumer. It allows the consumers to equip resources as per their demand. It allows the users to deploy their applications or software services effectively and they may access resources with all their rights. In IaaS, an organization leases out its resources to the consumer and the consumer pays back on per-use basis.

b.) Platform as a Service (PaaS):

PaaS is the layer that lies above the IaaS in the stack. It deals with providing development as well as deployment options to the consumers. It basically provides an environment for developing the application with some built-in tools which have some pre-defined functions which help the user to build the application as per requirement. Also, once the application is developed, it may be deployed within the same environment. But, the application so developed becomes environment specific and cannot be run on any other vendor's environment. It also supports the feature of renting of resources and the consumers have to pay on per-use basis.

c.) Software as a Service (SaaS) :

SaaS is the topmost layer in the stack and lies above the PaaS layer. It provides deployment of the end product or software or some web application on the IaaS and PaaS services and provides access to different consumers through some network, probably Internet nowadays. The services of this layer are perceived and manipulated by the consumers. The consumers access these services through Internet once the software has been deployed. The license to these services may be subscription based or usage based. The consumer may extend the services (subscription as well as scalability) based on the demand.

2 Literature Survey

A.) Sanjoli and Jasmeet [7], "Cloud data security using authentication and encryption technique", propose blend of two cryptographic algorithms, EAP-CHAP(Extensible Authentication Protocol- Challenge Handshake Authentication Protocol) and Rijndael Encryption Algorithm. EAP is used to provide authenticated access to the cloud environment. CHAP, a method of EAP, is implemented for authentication purpose. This is then followed by encryption using Rijndael Encryption Algorithm. The complete methodology involves few steps. In the first step, Cloud Service Provider (CSP) receives an authentication request from the user. In the second step, CSP sends acknowledgement after verifying the user identity using EAP-CHAP. In the third step, once the user is authenticated, the user encrypts the data using Rijndael Encryption Algorithm and uploads the encrypted data on to the server of CSP. The data is saved in encrypted form on to the server. Hence, when the user receives any encrypted data from CSP, it can be decrypted using same key same as that used for encryption. In this paper, client side security has been focused and encryption is in the hands of user for providing better security.

B.) Shirole and Sanjay[6], "Data Confidentiality in Cloud Computing with Blowfish Algorithm", propose a system that uses encryption technique to provide reliable and easy way to secure data for resolving security challenges. Scheduler performs encryption on plain data into cipher data followed by uploading of ciphered data on the cloud. When the data is to be retrieved from the cloud, it is obtained in plain data format and is stored on the system. This preserves data internally. And hence, this builds a relationship of cooperation between operator and service provider. This model uses OTP(One-Time Password) for authentication purpose and Blowfish algorithm for encryption purpose.

C.) Garima and Naveen [5], "Triple Security of Data in Cloud Computing", state that cloud computing is a networking model which is connected to a number of servers and is based on client server architecture providing various facilities due to its flexible infrastructure. According to this paper, since cloud computing is internet based technology, so, security stands as a major concern and introduce a mechanism to protect the data in the cloud using combination of two cryptographic algorithms and steganography. This paper proposes blend of two cryptographic algorithms viz.a.viz., DSA(Digital Signature Algorithm) and AES(Advanced Encryption Standard) and Steganography. DSA is used for authentication purpose, AES is used for encrypting the data and Steganography is used for further encryption. The working involves signing of the data in the first step. The signature is generated by first applying a hash function on the data and this gives compact form of data which is called message digest. The message digest is then signed using sender's private key. Once the message is signed, the data is encrypted along with the signature using AES. Once encryption is completed using AES algorithm, the data is further encrypted using steganography. Steganography hides message along with another media which does attract the attention of the intruder and hence the data is protected. This complete mechanism is implemented on ASP.NET Platform and ensures to achieve authenticity, data integrity and security of data in the cloud. This paper concludes that time complexity of the complete mechanism is high since it is one by one process.

D.) Parsi and Sudha[4], "Data Security in Cloud Computing using RSA Algorithm", state that cloud computing is an emerging technology and is fast becoming the hottest area of research. To provide data security in cloud environment, RSA algorithm has been implemented to provide the same. RSA stands for Ron Rivest, Adi Shamir and Len Adleman. RSA is public key cryptography. In the proposed system, RSA is used for both encryption and decryption of data. The process involves encryption of data and then uploading it onto the cloud. For decryption of data, required data is downloaded from the cloud, cloud provider authenticates the user and then the data is decrypted. RSA is used to provide authenticated access to intended user only and hence makes the system secure. The working of RSA consists of two keys: public key and private key. Public key is distributed and shared with others while the private key is only available with the original data owner. Thus, Cloud Service Provider(CSP) perform the encryption and decryption is performed by the consumer or cloud user. Hence, once the data is encrypted using public key, private key must be known in order to decrypt the data. RSA algorithm has three steps: Key Generation, Encryption and Decryption. Key generation is done between CSP and user and then encryption and decryption are performed further. The proposed system provides authenticated access and prevents any intruder access. Hence, the system is made secure.

3 Proposed Work

The hybrid algorithm that has been implemented is a combination of two popular and most widely used cryptographic symmetric and asymmetric algorithms viz.a.viz., RSA as Digital Signature and Blowfish Algorithm. RSA as Digital Signature is used for authentication and verification purpose and Blowfish is used for encryption and security purpose.

RSA was introduced by Ron Rivert,Adi Shamir and Leonard Adleman in 1977. Initials of their names has been used to name the popular algorithm, RSA.

RSA falls under public key cryptography. RSA as Digital Signature aims at providing authentication and non-repudiation of the message. It means that the message that the receiver receives is received from the intended sender and also the message is not duplicated.

Two keys are used for signing the document: public key and private key. The private key, as the name suggests, is kept secret with the sender and is not shared globally and hence is used for signing the document. The public key is shared globally and is used for authentication of the sender by receiver. The working of RSA as Digital Signature has following steps:

- a.) Firstly a message digest of the document is prepared using the hash function.
- b.) Signing of the document is performed using the private key generated using RSA algorithm.
- c.) Verification of the document is performed using the public key generated using RSA algorithm.

Once the document is signed, further encryption is performed by Blowfish algorithm in order to make a secure system.

Blowfish algorithm, was introduced by Bruce Schneier in 1993, is a very famous fast secret key cryptography. The working of this algorithm is complex and is hard to be broken by any intruder. This will make the system secure and will prevent any breach of security. Blowfish has a block size of 64-bit and a variable key length which varies from 32 bits up to 448 bit. The process has 16-round Feistel cipher and large key-dependent S-boxes are used for encryption/decryption purpose. The working includes of following steps:

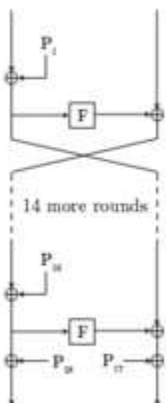


Fig. 1 The Feistel structure of Blowfish

- a.) The diagram above is pictorial representation of Blowfish. Each row represents 32 bits.

b.) The algorithm uses two subkey arrays: the 18-entry P-array and four 256-entry S-boxes.

c.) The S-boxes take 8-bit input and give 32-bit output.

d.) In every round, an entry from P-array is taken, and after the final round, each half of the data block is XORed with one of the two remaining unused P-entries.

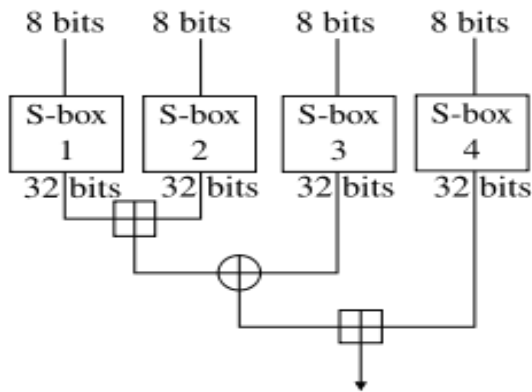


Fig. 2

e.) The diagram above shows Blowfish's F-function.

- Firstly, the input is divided into four eight-bit quarters.
- These quarters are then given as input to the S-boxes.
- The outputs are added modulo 2^{32} and XORed and a final output of 32-bit are obtained.

f.) Decryption is performed using these steps, except that P1, P2, ..., P18 are used in reverse order.

4 Working Of Hybrid Algorithm

The Proposed Algorithm consists of blending of two algorithms: RSA as Digital Signature and Blowfish Algorithm. RSA as Digital Signature provides non-repudiation and authentication of the document while Blowfish is used for encryption and decryption purpose. Once the document is signed and encrypted using the hybrid algorithm, two copies of digital signature are created out of which one is stored locally and another is uploaded onto the cloud along with encrypted message. For decryption, document will be decrypted using Blowfish and then digital signatures are matched with the copy of digital signature stored onto cloud.

Step1. Key Generation Algorithm using RSA

Public key and private key will be generated using RSA algorithm.

The steps for RSA algorithm are:

- Choose two distinct large random prime numbers p and q .
- Find $n = pq$, where n is the modulus for public and private keys.
- Find the totient: $\phi(n) = (p-1)(q-1)$.
- Choose an integer e such that $1 < e < \phi(n)$, and e and $\phi(n)$ have no factors other than 1, where e is declared as the public key exponent.
- Find d to satisfy the congruence relation $d \times e = 1$ modulus $\phi(n)$; d is the private key exponent.
- The public key is (n, e) and the private key is (n, d) . All the values d, p, q and ϕ must be kept secret.

Step2. Generation of Digital Signature

- Before signing the document, the sender creates a message digest using a hash function.

- b.) Message digest is basically a crushed form of entire message and so any hash function may be used for creating the message digest.
- c.) Once the message digest M , is created it may be used for signing the document using private key.
- d.) The private key (n,d) is used to sign the document using $S=M^d \text{ mod } n$.
- e.) After the document is signed, the document is further encrypted.

Step3. Encryption of the document

- a.) Once the document is signed, it is ready to be encrypted.
- b.) For encryption, Blowfish algorithm is used.
- c.) It has 16 round Feistel structure and key dependent S-boxes.
- d.) Basic operation performed in this algorithm is XOR logic function.
- e.) XOR operation is performed on the output of each row.
- f.) After 16 rounds of XOR operation, the encryption process is complete.

Step4. Decryption of the document

- a.) The decryption process is achieved using reverse of Blowfish algorithm.
- b.) This process gives the message digest generated during digital signing of the document.

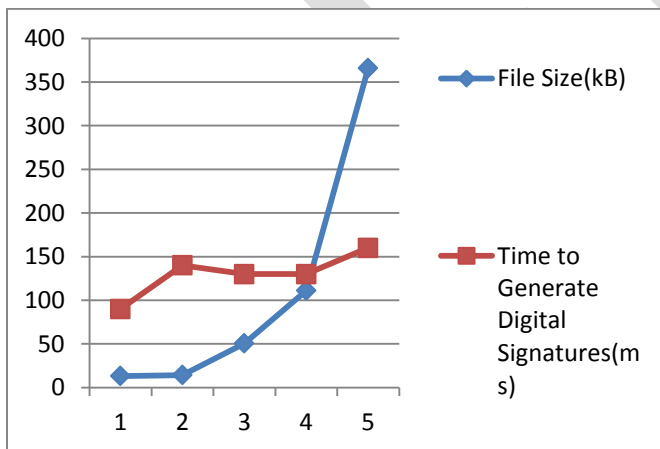
Step5. Verifying the Digital Signature

- a.) The receiver verifies the sender by matching the digital signatures obtained after decryption with that saved onto the cloud.
- b.) If the signatures match, the sender is verified.

5 Results

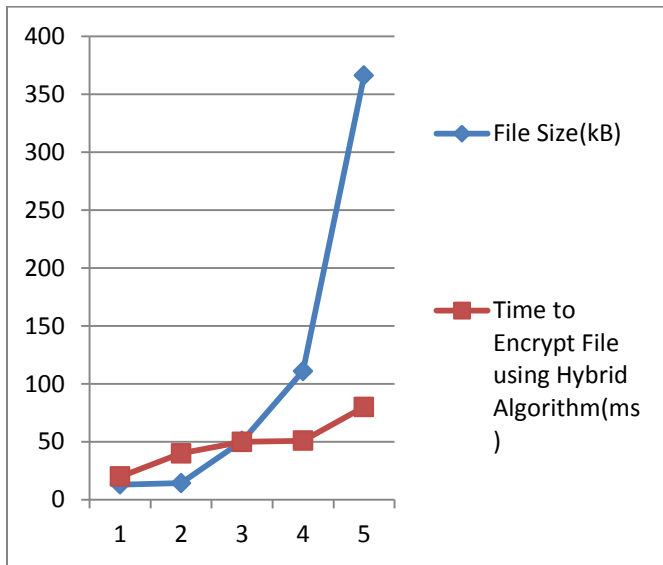
The algorithm is implemented using Java NetBeans and results have been simulated using CloudSim. Following results have been obtained for different file sizes.

a.) Time to Generate Digital Signatures



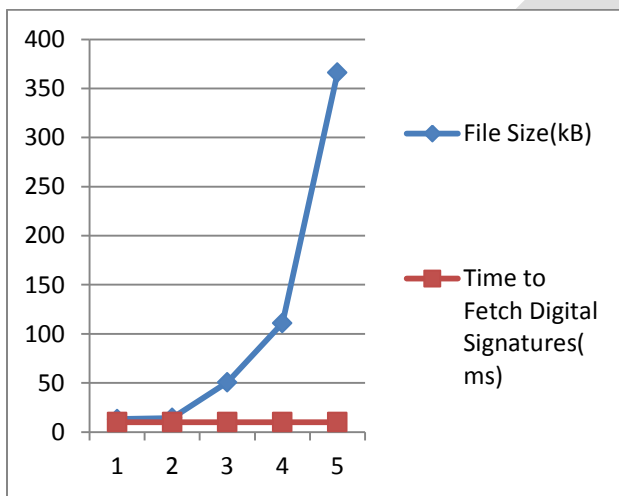
Time to generate digital signatures varies proportionally with file size. As the file size increases so does the generation time increases.

b.) Time to Encrypt Message using Hybrid Algorithm



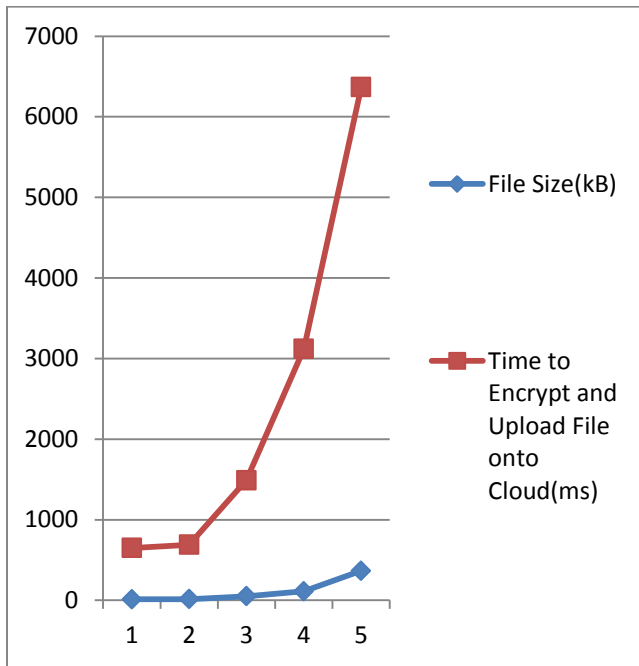
Time to encrypt file using hybrid algorithm varies proportionally with file size. As the file size increases so does the encryption time increases.

c.) Time to Fetch Digital Signatures from Cloud



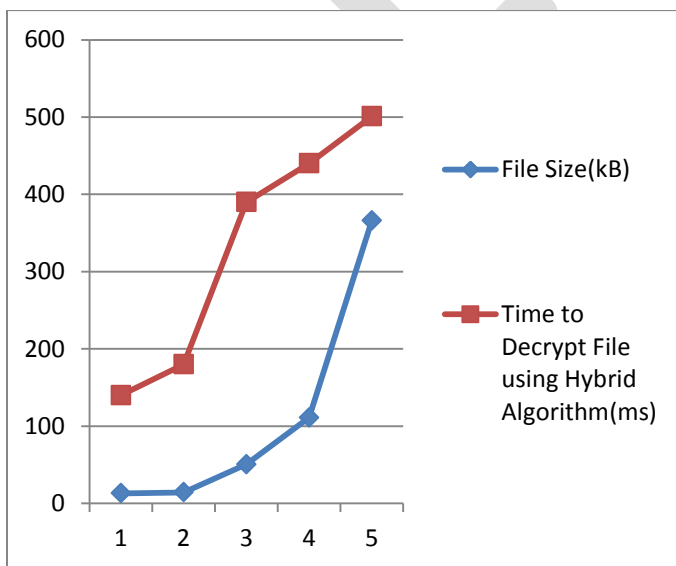
Time to fetch digital signatures is independent of file size. It remains constant for all file sizes.

d.) Time to Encrypt and Upload File onto Cloud



Time to encrypt and upload file onto cloud varies proportionally with file size. As the file size increases, encryption and upload time increase.

e.) Time to Decrypt File



Time to decrypt file is directly related to file size. As file size increases, decryption time increases.

6 Conclusions

The implemented algorithm is a hybrid of two algorithms. From above results, it can be concluded that new Hybrid Algorithm is fast since it takes few milliseconds to encrypt and decrypt the message. Also, it is secure since the encrypted code cannot be understood easily. This is advantageous as it makes the new algorithm secure and fast too. Blending of these two algorithms has fetched the better of two worlds of public key cryptography and secret key cryptography.

REFERENCES:

- [1] http://en.wikipedia.org/wiki/Category:Cloud_computing_providers
- [2] <http://www.cloudcomputingchina.cn/Article/luilan/200909/306.html>
- [3] http://searchcloudcomputing.techtarget.com/sDefinition/0, sid201_gci1287881,00.html
- [4] Kalpana, Parsi, and Sudha Singaraju. "Data security in cloud computing using RSA algorithm." *IJRCCT* 1.4 (2012): 143-146.
- [5] Saini, Garima, and Naveen Sharma. "Triple Security of Data in Cloud Computing." *International Journal of Computer Science & Information Technologies* 5.4 (2014).
- [6] Subhash, Shirole Bajirao. "Data Confidentiality in Cloud Computing with Blowfish Algorithm." *International Journal of Emerging Trends in Science and Technology* 1.01 (2014).
- [7] Singla, Jasmeet Singh. "Cloud data security using authentication and encryption technique." *Global Journal of Computer Science and Technology* 13.3 (2013).
- [8] Naik, Uma, and V. C. Kotak. "Security Issues with Implementation of RSA and Proposed Dual Security Algorithm for Cloud Computing."
- [9] Somani, Uma, Kanika Lakhani, and Manish Mundra. "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing." *Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on.* IEEE, 2010.
- [10] Hashizume, Keiko, et al. "An analysis of security issues for cloud computing." *Journal of Internet Services and Applications* 4.1 (2013): 1-13.
- [11] Rani, Sunita, and Ambrish Gangal. "Cloud security with encryption using hybrid algorithm and secured endpoints." *International journal of computer science and information technologies* 3.3 (2012): 4302- 4304.
- [12] Saravanan, N., et al. "An implementation of RSA algorithm in google cloud using cloud SQL." *Research Journal of Applied Sciences, Engineering and Technology* 4.19 (2012): 3574-3579.
- [13] <http://cloudcomputingcafe.com/>
- [14] Devi, G., and M. Pramod Kumar. "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm." *International Journal Of Computer Trends And Technology* 3.4 (2012): 592-596.
- [15] Kaur, Randeep, and Supriya Kinger. "Analysis of Security Algorithms in Cloud Computing."
- [16] Thakur, Jawahar, and Nagesh Kumar. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis." *International journal of emerging technology and advanced engineering* 1.2 (2011): 6-12.
- [17] Kumar, K. Vijay, Dr N. Chandra Sekhar Reddy, and B. Srinivas Reddy. "Preserving Data Privacy, Security Models and Cryptographic Algorithms in Cloud Computing." *International Journal of Computer Engineering and Applications* 7.1 (2015).
- [18] Kaur, Jasleen, et al. "SURVEY PAPER ON SECURITY IN CLOUD COMPUTING." (2015).
- [19] Kaur, Jasleen, and Sushil Garg. "Security in Cloud Computing using Hybrid of Algorithms."