International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October, 2015
ISSN 2091-2730

Security in Cloud Computing using Hybrid of Algorithms

Jasleen Kaur[1], Dr. Sushil Garg[2]
[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 is a metaphor for network that provides its services such as dynamic resource pools, high availability and virtualization using Internet know as Cloud Computing. Cloud Computing provides resources to the users over internet as per their demand. Service on demand is an important feature of cloud computing as it enables the user to pay for the required resources only. There are many Cloud Service Providers (CSP) such as Google, Microsoft, IBM, Oracle Corporation, Amazon Web Services, etc. which provide cloud services to users. Since cloud computing involves sending data over internet, security breach needs to be monitored and controlled. So, this paper introduces a new hybrid algorithm which is blend of two cryptographic algorithms: public key cryptography and secret key cryptography. This new algorithm is hybrid of RSA as Digital Signature and Blowfish Algorithm and will provide security to the data while being uploaded or downloaded from cloud.

Keywords- Cloud Computing, Security, Deployment Models, Service Models, Security, RSA as Digital Signature, Blowfish Algorithm

1 INTRODUCTION

Cloud Computing is internet based technology which has evolved in the field of IT over the past few years. Cloud computing makes the transfer or storage of bulk data easy to be transferred and maintained for usage. Organizations need not buy special hardware for deploying different applications since cloud computing provides with pay-as-you-go pricing basis which means that all the resources like firewall, server, database and so on that are required by an organization for the deployment of an application may be leased out by some other organization which deals in providing those resources. The latter organizations are known as cloud vendors. Hence leasing out of resources does not levy high cost on the users and at the same time it gives business to other people as well. So, cloud computing is fast becoming popular in the field of IT and is gaining attention of various organizations.

Some of the famous cloud providers are:

A. Google: Google provides internet services for storing and accessing the data as and when required. It provides various services such as mailing, storing of various documents, translation, sharing of documents to selected users, etc. The most commonly used service of Google is Google Drive which is used for sharing of personal data through internet.

B. Microsoft: Microsoft provides internet services for file sharing and storing through its office applications. Microsoft Cloud storage patents are Microsoft Azure and OneDrive for storing enormous data and then accessing it from any location.

C. Salesforce.com: Salesforce provides online services for sales, support and businesses through remote access from any location and at any time.

Figure: Cloud Computing

1.1 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.

1.2 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.

2 LITERATURE SURVEY

A.) Sanjoli and Jasmeet [7], "Cloud data security using authentication and encryption technique", state that cloud computing is an internet based technology that will provide everything as service on demand . This paper proposes 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.

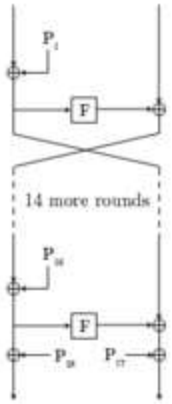
D.) Parsi and Sudha[4], "Data Security in Cloud Computing using RSA Algorithm", state that cloud computing is an emerging technology and is fast becoming the hottest area of research. Cloud computing is effective in reducing the costs and provides on demand services to the users. Since cloud computing is based on the concept of open environment, security stands as a hindrance to the deployment of cloud environments. 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 encryption as well as decryption of data. The process involves that the data is encrypted and then uploaded onto the cloud. For decryption of data, data required 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 proposed work is based on blending two popular encryption algorithms viz.a.viz., RSA as Digital Signature and Blowfish algorithm.
RSA was introduced by Ron Rivert,Adi Shamir and Leonard Adleman in 1977. RSA has been named using initials of their names.
RSA is public key cryptography. RSA as Digital Signature is used for authentication and non-repudiation purpose. It makes sure that the message is received from the desired sender. For signing the document or message, two keys are required: public key and private key. The private key, as the name suggests, is not shared with anyone and hence is used for signing the document. The public key is known to all and is used to authenticate the sender. The working of RSA as Digital Signature has following steps:
a.) Firstly, a hash function is framed to create the message digest.
b.) For encryption, the private key generated using RSA algorithm is used to sign the document.
c.) For decryption, the public key generated using RSA algorithm is used to verify the document.

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

Blowfish algorithm is a very popular and fast secret key cryptography. It was introduced by Bruce Schneier in 1993. The encryption/decryption process of this algorithm is complex and cannot be broken by any intruder. So, it will make the system secure. Blowfish consists of a 64-bit block size and a variable key length which varies from 32 bits up to 448 bit. The process is a 16-round Feistel cipher and large key-dependent S-boxes are used. The working includes of following steps:



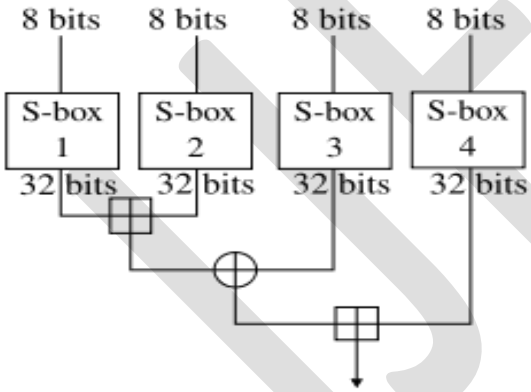
The Feistel structure of Blowfish

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.



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

- Firstly, the input is split into four eight-bit quarters
- these quarters are then 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 the steps, except that P1, P2,..., P18 are used in reverse order.

4 WORKING OF PROPOSED ALGORITHM

The Proposed Algorithm consists of hybridization of two algorithms: RSA as Digital Signature and Blowfish Algorithm. Digital Signature will provide authentication and non-repudiation to the data while Blowfish will be used for encryption/decryption. Once the document is signed and encrypted using the hybrid algorithm, it will be uploaded onto the cloud provided by Cloud Service Providers (CSP). For decryption, document will be downloaded and then decrypted after authentication using public key.

Step1. RSA Key Generation Algorithm

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

The steps for RSA algorithm are:

a.) Choose two distinct large random prime numbers p and q.
b.) Find n = pxq, where n is the
modulus for public and private keys.
c.) Find the totient: $\phi(n) = (p-1)(q-1)$.
d.) 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.
e.) Find d to satisfy the congruence
relation $d \times e = 1$ modulus $\phi(n)$; d is the private key exponent.
f.) The public key is (n, e) and the private
key is (n, d). All the values d, p, q and
phi must be kept secret.

Step2. Digital Signature

a.) 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 $S=M^d \bmod n$.
e.) After the document is signed, the document is further encrypted.

Step3. Encryption

a.) Once the document is signed, it is ready to be encrypted.
b.) For encryption, Blowfish algorithm is used.
c.) It has 16 round Fiestel 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

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 Sender

a.) The receiver verifies the sender by using the public key of the sender.
b.) Receiver uses sender's public key (n, e) to compute integer $V=S^e \bmod n$.
c.) Receiver extracts the message digest from the integer V.
d.) Then, receiver independently computes the message digest of the information that has been signed.
e.) If both message digests are identical, the sender is valid.

5CONCLUSION

Cloud computing is fast becoming popular in IT field and is being adopted by every organization in order to keep their data all at one place. So, keeping the data secure is an important aspect of cloud computing. The new hybrid algorithm will provide security of data. RSA as Digital Signature will provide authenticity and non-repudiation to the data while Blowfish algorithm will provide security as it will encrypt the data. Also, the chances of breach in this hybrid algorithm will be quite less as the encryption process of Blowfish

algorithm is complex and cannot be broken easily and RSA as Digital Signature will make sure that the data is from a valid sender only. So, the hybrid algorithm aims at securing the very sensitive data of every organization that will be uploaded onto the cloud.

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)