Open access Journal International journal of Emerging Trends in Science and Technology

Data Confidentiality in Cloud Computing with Blowfish Algorithm

Shirole Bajirao Subhash' Dr Sanjay Thakur
Student, CSE, Lord Krishna College of Technology, Indore, India
Asso.Prof. CSE, Lord Krishna College of Technology, Indore, India
Email: baji_shirole@yahoo.com

Abstract: - Cloud provides enormous capacity of storage for cloud users. It is more reliable and flexible to users to store and retrieve their data at anytime and anywhere. It is an increasingly growing technology. Nowadays, many enterprises have started using cloud storage due to its advantages. Even though the cloud continues to gain popularity in usability and attraction, the problems lie in data security, data confidentiality, privacy and other data protection issues. Security and Confidentiality of data stored in the cloud are major setbacks in the field of Cloud Computing. Security and Confidentiality are the key issues for cloud storage. This paper proposes a Blowfish encryption algorithm to address the security and Confidentiality issue in cloud storage in order to protect the data stored in the cloud.

Keywords: Cloud Storage, Security, Confidentiality, Encryption Algorithm, Cryptography

1. Introduction

Cloud computing is the collective term for a group of IT technologies which in collaboration are changing the landscape of how IT services are provided, accessed and paid for. Some of the supporting technologies have already been available for quite some time, but it is the combination of several technologies which enables a whole new way of using IT. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The above definition is by no means exhaustive and it is very hard to find two experts having the same definition of cloud computing. Cloud computing is still an evolving paradigm. The characteristics, deployment and delivery models, as well as the underlying risks, technologies, issues and benefits will be refined by energetic debate by both the public and the private sectors. As with most new technologies and paradigms, one tends to look for the functionality first and only later on, one looks after the security of such functionality. However, cloud computing raises such an amount of questions concerning security guarantees that potential users are waiting for clear answers before moving into the cloud. Cloud is the combination of work of server and connections. It is easy to access information stored in the cloud. Cloud computing collects all the computing resources and software required to work on them. It provides an efficient technique to provide an accurate information and proper service to users and enterprises. Cloud computing is also described as "On-demand computing" because the user can access as per their requirement and demand.

2. Characteristics of Clouds

2.1 Rapid elasticity

The cloud computing resources can rapidly match with the increasing cloud capabilities if the demand increases.

2. 2 Measured service

It enables the measuring of used resources similar to the utility computing.

2.3 Resource pooling

This resource pool helps in enabling the use of physical and virtual resources by multiple users.

2.4 Broad network access

Cloud services are available on any kind of network.

2.5 On Demand Self-service

Cloud Computing resources can be obtained and disposed of by the consumer without human intervention among cloud service providers.

3. Cloud Service and Deployment Models

3.2 Software-as-a-Service (SaaS)

SaaS is one of the oldest and nature domains of cloud computing. SAAS is nothing but a software distribution model, which is available to customers over a network such as server or internet. SaaS is an interface between cloud applications and customers to offer them on demand network.

3.2 Platform-as-a-Service (PaaS)

Platform as a service provides high-level environment to design, build, test, deploy and update online cloud applications. PaaS is a paradigm which mainly deals for delivering operating systems and other services over the internet. PaaS provides solutions for developing as well as deploying applications over internet such as operating system and virtualized servers.

3.3 Infrastructure-as-a-Service (IaaS)

Infrastructure as a service is equipment that used to support hardware, software, storage, servers and mainly used for delivering software application environments. It totally depends on pricing model. IaaS companies provide off line server, storage and networking hardware as permanent basis and can be access over the Internet. So it becomes easier to get access to run their applications on this hardware anytime without wasting office space

4. Cloud Deployment Models

4.1 Public Cloud

A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.

4.2 Private Cloud

A private cloud is established for a specific group or organization and limits access to just that group.

4.3 Community Cloud

A community cloud is shared among two or more organizations that have similar cloud requirements.

4.4. Hybrid Cloud

A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community.

5. System Task Dimension about Confidentiality

5.1 Transfer

Disclosure of sensitive data during transfer from one party to the other is a concern that has been addressed quite extensively with the use of encryption.

5.2 Storage

When the data is stored outside the direct control, the data owner can exercise separation of duties, by encrypting the data before storing it externally, while keeping the means of decryption in the owner's control.

5.3 Processing

Processing refers to any use or transformation of data. When processing needs to take place within the cloud, data cannot be protected by the same means as data at rest and data in transit (e.g. encryption).

6. The Cloud Security Solutions

6.1 System Solution

To achieve the security requirements it directly manipulates the hardware and the software. They provide the security at the lower levels of the technology stack. The solution such as encryption i.e., cryptography act as a base for the behavioural solutions. Another system solution techniques IDS (Intrusion Detection system), detects the security breaches by monitoring the data transfers and execution of functionality.

6.2 Behavioural solutions

These act on the higher level of abstraction. They focus on the behaviour of the users in the information system.it is formed on the basis of the trust based solutions i.e., information to only trusted and the policy based solutions i.e., limit the users access to the information resources.

6.3 Hybrid solutions

It comprises a combination of the system and behavioural solutions indicating both authentication and authorization.

7. Proposed System

In proposed system resolves security challenges for data in the cloud and provides a reliable and easy way to secure data with encryption technology. In this system, the customer will get a proof of integrity of the data that he or she wishes to store in the cloud with bare minimum costs and efforts.

Encryption process is performed with the help of scheduler which will encrypt the plain data into cipher data and that ciphered data is uploaded on cloud. At the time of retrieval the ciphered data is again retrieved into plain data which is stored on system. This reduces the chances of getting discloser internally. In this manner, a relationship is established to cooperation model between operator and service provided to the users.

Here the proposed modules describes are as follows

- ERP System
- OTP required scheduling the data
- Encryption/Decryption
- Data Transfer to cloud
- SOAP Protocol
- Retrieve the data from cloud
- Compare the Data

7.1 ERP System

User may be an ERP system or business organizations who use cloud for data storage. An ERP system runs on a variety of computer hardware and network configurations, typically employing a database as a repository for information. The transformation of ERP into a cloud-based model has been relatively slow some functionality is being moved to the cloud for data storage and computation.

7.2 One Time Password

One time password is required to schedule the data on the cloud. When OTP is required we have to send the Message from system only. OTP will come to Email ID & enter that OTP in system then it enable scheduler option to transfer the data on cloud. Schedule button schedule the data on cloud with blowfish encryption.

7.3 Encryption/Decryption

This system will accept normal data then it will encode the given data, after encoding it will provide encrypted data in cipher text, which is processed as this system deals with the database of ERP or organization's transactional data in real time, such as encrypted fields, records, rows, or column data in a database. Once encryption is done then that cipher text will be deciphered by CSV Parser. It will provide security to data, so that no unauthorized user can view, modify, delete the data of ERP. For encryption process blowfish algorithm is used.

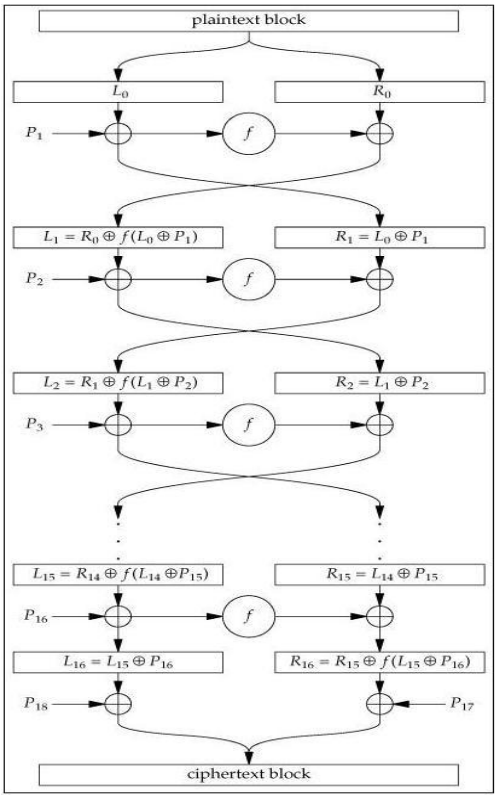
7.4 Blowfish Algorithm

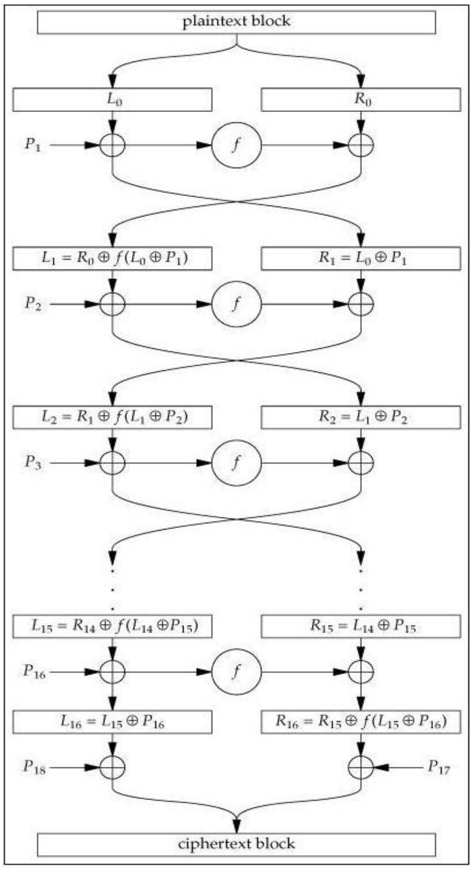
Blowfish was designed by Bruce Schneier as a fast, free alternative to existing encryption algorithms. It is easiest and fastest algorithm for encryption. Blowfish is a variable-length key block cipher. It is significantly faster than DES when implemented on 32-bit microprocessors with large data caches, such as the

Pentium and the PowerPC. For bulk encryption this algorithm is efficient in encrypting data files or a continuous data stream. Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Blowfish uses a large number of sub keys. These keys must be pre computed before any data encryption or decryption.

7.5 Encryption Process

Blowfish is a Feistel network consisting of 16 rounds. The input is a 64-bit data element, Steps for Blowfish algorithm is as shown below. In this, a 64-bit plaintext message is first divided into 32 bits. The "left" 32 bits are XORed with the first element of a P-array to create a value I'll call P', run through a transformation function called F, then XORed with the "right" 32 bits of the message to produce a new value I'll call F'. F' then replaces the "left" half of the message and P' replaces the "right" half, and the process is repeated 15 more times with successive members of the P-array. The resulting P' and F' are then XORed with the last two entries in the P-array (entries 17 and 18), and recombined to produce the 64-bit cipher text.


plaintext block
L_0
R_0
P_1
f
$L_1 = R_0 \oplus f(L_0 \oplus P_1)$
$R_1 = L_0 \oplus P_1$
P_2
f
$L_2 = R_1 \oplus f(L_1 \oplus P_2)$
$R_2 = L_1 \oplus P_2$
P_3
f
$L_{15} = R_{14} \oplus f(L_{14} \oplus P_{15})$
$R_{15} = L_{14} \oplus P_{15}$
P_{16}
f
$L_{16} = L_{15} \oplus P_{16}$
$R_{16} = R_{15} \oplus f(L_{15} \oplus P_{16})$
P_{18}
P_{17}
ciphertext block


plaintext block
L_0
R_0
P_1
f
$L_1 = R_0 \oplus f(L_0 \oplus P_1)$
$R_1 = L_0 \oplus P_1$
P_2
f
$L_2 = R_1 \oplus f(L_1 \oplus P_2)$
$R_2 = L_1 \oplus P_2$
P_3
f
$L_{15} = R_{14} \oplus f(L_{14} \oplus P_{15})$
$R_{15} = L_{14} \oplus P_{15}$
P_{16}
f
$L_{16} = L_{15} \oplus P_{16}$
$R_{16} = R_{15} \oplus f(L_{15} \oplus P_{16})$
P_{18}
P_{17}
ciphertext block

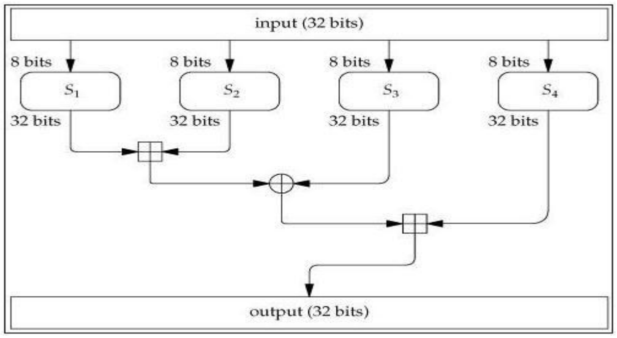
Blowfish Encryption

```
Divide x into two 32-bit halves: xL, Xr
For i = 1to 16:
    xL = XL XOR Pi
    xR = F(XL) XOR xR
    Swap XL and xR
Swap XL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR
```

7.6 Function

The function is arguably the most complex section of the algorithm and the only section that uses the S-

Boxes. The F function accepts a 32 bit stream of data and divides the input into four equal sections. Each 8 bit subdivision is transformed into a 32 bit data stream by means of their corresponding S-Box. The resulting 32 bit data is XOR'ed or added together to provide a final 32 bit value for further permutations of the Blowfish algorithm, see Figure for details (note that all addition is modulo 232).



Representation of Function

7.7 Decryption Method

Decryption is exactly the same as encryption, except that P1, P2... P18 are used in the reverse order. Implementations of Blowfish that require the fastest speeds should unroll the loop and ensure that all sub keys are stored in cache.

7.8 SOAP Protocol

SOAP originally defined as “Simple Object Access Protocol” is a protocol specification for exchanging structured information in the implementation of web services in computer networks. It relies on Comma separated values (CSV) files for its message format and usually relies on other application layer protocols. This SOAP protocol is used for interfacing with Cloud Service Provider (CSP).The main idea behind SOAP was to:

a. Improve Internet interoperability

b. Integrate various business systems

7.9 Retrieve the data from cloud

CSV Parser is used for deciphering the text. It defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It maintains the layout of CSV Files’ without change, while uploading on cloud. It is used when data is retrieved from the cloud to use. CSV Parser required to retrieve the data from cloud Compare the Data on the cloud with original data.

7.10 Compare the Data

An optional Compare who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request. Compare should be able to efficiently audit the cloud data storage without local copy of data and without bringing in additional on-line burden to users. Also Compare will give alerts to users whenever some other person tries to attack data or unauthorized access to data in cloud storage.

8. Conclusion

The three data security objectives (Confidentiality, Integrity, and Availability (CIA)). For securing the database of ERP on cloud with the help of encryption and SAOP protocol. It has become easy to encrypt as well as upload data simultaneously on cloud on one click only that is scheduling. The data which is visible to user on CSP is in Encrypted form. So here the hacker could not understand what exact is the information about or which record it is. Comparison of data is done if a change which gives alert sending message (Email) on Email Id.

References

[1]International Journal of Advanced Research in Computer and Communication EngineeringVol. 2, Issue 8, August 2013 Dr. L. Arockiam1, S. Monikandan2

[2] IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814 Mohit Marwaha1, Rajeev Bedi2

[3] International Association of Scientific Innovation and Research (IASIR) Rashmi Nigoti1, Manoj Jhuria2 Dr.Shailendra Singh3

[4] JECET; June – August-2013; Vol.2.No.3, 883-888. Jitendra Singh Rajawat1 and Sanjay Gaur2

[5] AN OVERVIEW OF THE SECURITY CONCERNS IN ENTERPRISE CLOUD COMPUTING by Anthony Bisong and Syed (Shawon) M. Rahman at International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011

[6] Cloud Security Alliance: Security Guidance Critical Areas of Focus in Cloud Computing, http://www.cloudsecurityalliance.org/guidance/csaguide.pdf. April 2009.

[7] Cloud computing and Confidentiality, W. Pieters and Prof. Dr. P.H. Hartel, University of Twente.s

[8] Management and Security for Grid, Cloud and Cognitive Networks by Carlos B. Westphall, Carla M.Westphall,FernandoL.Koch: http://www.fsma.edu.br/si/sistemas.html

[9] Enhancing Security in Cloud computing using Public Key Cryptography with Matrices Birendra Goswami & Dr. S. N. Singh: www.ijera.com Vol. 2, Issue 4, July-August 2012

[10] Improving the Security of Cloud Computing using Trusted Computing Technology by P. Senthil, N. Boopal & R. Vanathi : www.ijmer.com Vol.2, Issue.1, Jan-Feb 2012.

[11] http://en.wikipedia.org/wiki/Cloud_computing

[12] http://www.techno-pulse.com/ Cloud Computing for Beginners

[13] Security and Privacy in Cloud Computing (Lecture 1, 01/25/2010) by Ragib Hasan at Johns Hopkins Universityen.600.412

[14] USCERT-Cloud Computing Huth Cebula

[15] ttp://en.wikipedia.org/wiki/Trusted_Computing