International Journal for Rapid Research in Engineering Technology & Applied Science
Vol IV Issue VII 07 2018
ISSN (Online): 2455-4723

Design and Implementation of Snort-J48 Algorithm Based Intrusion Detection on public cloud

Rahul Yadav, Mohit Jain
Department of Computer Science & Engineering, BM College of Technology, Indore, M.P, India
ryadavmtech@gmail.com,bmctmohitcs@gmail.com***

Abstract: In the cloud environment, resources, servers and users are shared among all of the individuals. So it is difficult for cloud providers to ensure file safety. Consequently if an intruder, use and misuse the data, it is basically very easy to destroy. Cloud computing security key issues are which focuses on the development of cloud computing security solutions encyclopedia This thesis using Blowfish algorithm and hash data security, authentication, and integrity of files is able to solve problems on the cloud secure file exchange is present in reducing cloud. Cryptography algorithms improve data security. In our system, we enhanced symmetrical, asymmetrical and hash algorithms, which provide better results for unified performance standards.

Keywords: Hybrid Cryptosystem, Blowfish, File Splitting, Cloud Security.

I Introduction

Cloud computing is originated from earlier large-scale distributed computing technology. NIST [1] defines Cloud computing as "A model for enabling convenient, on demand network access to a shared pool of configurable computing resources(e.g. , networks ,storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". In Cloud computing, both files and software are not fully contained on the user's computer. File security [2] concerns arise because both user's application and program are residing in provider premises. The cloud provider can solve this problem by encrypting the files by using encryption algorithm. This paper presents a file security model to provide an efficient solution for the basic problem of security in cloud environment. In this model, hybrid encryption is used where files are encrypted by blowfish coupled with file splitting and is used for the secured communication between users and the servers.
TPA at the client side and on the server, we calculate the hash value of the hash function, as well as compare the main server. In this scheme, data encryption is used to protect against the transmission. Because the encrypted file is stored on the cloud, users can be confident that his / her data is safe. Only channels, which reduces the problem of information disclosure on the transfer of files in encrypted form.

A. Blowfish

Blowfish is an encryption algorithm [3] that can be used as a replacement for the DES or IDEA algorithms. It is a symmetric block cipher that uses a variable length key, from 32 bits to 448 bits, making it useful for both domestic and exportable use

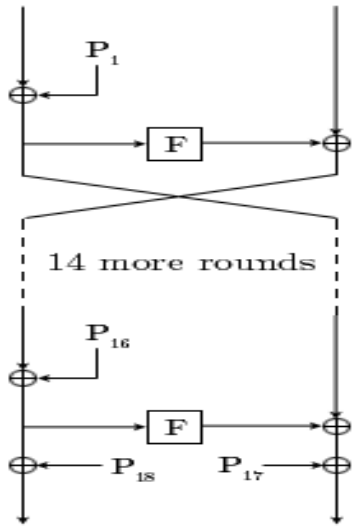

Fig.1 Representation of Blowfish Cryptographic Algorithm

The Feistel network of Blowfish algorithm is one that utilizes a structure that makes encryption and decryption very similar through the use of the following elements [2, 17]:

P box: Permutation box that performs bit shuffling.

box: Substitution box for nonlinear functions.

XOR: Logic function to achieve linear mixing.

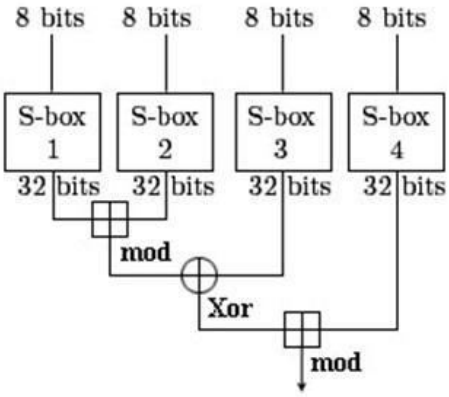

Fig.2 Representation of F function

Figure [3] shows a graphical representation of the F function, which has been shown as the most accessed function of the Blowfish algorithm

B. Digital Signature

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by sender. Block diagram of digital signature

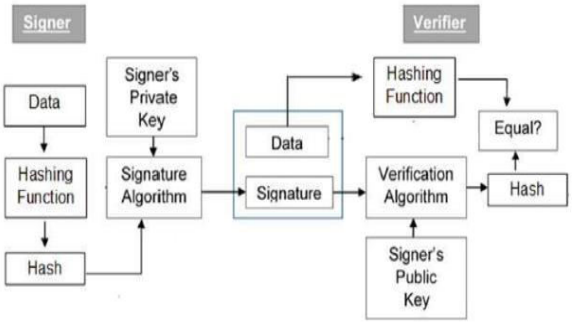

Fig.3 Representation of digital signature

Importance of digital signature is

- Message authentication
- Data Integrity
- Non-repudiation

II Problem Definition

In spite of its popularity, however, cloud computing has raised a range of significant security and privacy concerns which hinder its adoption in sensitive environments.

The transition to cloud computing model exacerbate security and privacy challenges, mainly due to its dynamic nature and the fact that in this model hardware and software components of a single service span multiple trust domains. In the cloud, data and services are not restricted within a single organization's perimeter. This dynamism and fluidity of data introduces more risk and complicates the problem of access control.

Layered architecture of cloud computing requires different levels of security considerations. In this work we are mainly concerned with the problem of identity management and access control in application and service level. We introduce a set of multi-party protocols specifically designed for cross-domain integrated cloud services. The main objective of these protocols is to provide more visibility and control to the end-users and close the gap between capabilities of existing solutions and new requirements of cloud-based systems.

III Proposed Methodology

In order to ensure file security on cloud, the above hybrid cryptosystem is deployed on cloud. We assume cloud server as trusted but in order to prevent tampering/misuse of data by intruder or data leakage or other security concerns, the data is stored at server in the encrypted form. We broadly classify the scheme deployed on cloud in three phases:

- Registration Phase
- Uploading Phase
- Downloading Phase

We used Open Shift toolkit to set up cloud environment. In Open Shift, we have one front node and n cluster nodes.

The VM's are deployed from front node to the corresponding cluster node Open Shift has been designed in such a way that it allows integration with many different hypervisors and environments. There is a front-end that executes all the process in open shift while the cluster nodes provide the resources that are needed by VM. There is at least one physical network joining all the cluster nodes with the frontend.

A. Registration Phase

In the Registration Phase, the client registers himself in order to upload and view his files to/from the cloud server .In the registration process, the client sends its request to front node and in return, front node assigns the VM of the

cluster node, which has minimum load among other VM's on the network to the client. At the end of registration phase, the client is registered with IP address of corresponding VM. Whenever he again issues his request, the request is transferred to its corresponding VM. The encrypted files, encrypted blowfish keys are stored at his registered VM.

B. Uploading Phase

In the Uploading Phase, steps are as follows:
Step 1:The client will send request to front node to authenticate himself.
Step 2:On successful authentication, the front end which send the corresponding IP address of the VM against which user was registered.
Step 3:The files are uploaded by the client to the registered server (VM).
Step 4: The encryption of uploaded files is done using the hybrid cryptosystem.
Step 5:The encrypted slices and Blowfish encrypted keys remain stored in VM's data store so that only the authenticated user is able to view his uploaded file.

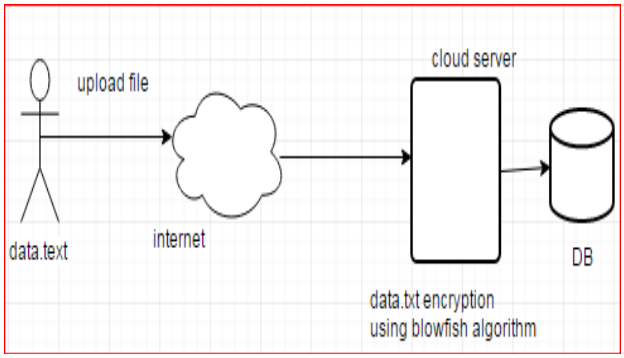

Fig. 4 Uploading Phase

C. Downloading Phase

In the downloading phase, the steps are as follows:
Step 1: The client will send request to front node to authenticate himself.

Step 2: On successful authentication, the front end which send the corresponding IP address of the VM against which user was registered.
Step 3: The client will upload n private keys for the corresponding n slices.
Step 4: The private keys will decrypt the corresponding encrypted Blowfish keys and the encrypted slices are decrypted by Blowfish keys.
Step 5: The decrypted files are merged to generate original file.
Step 6: The decrypted file is downloaded and viewed at client end.

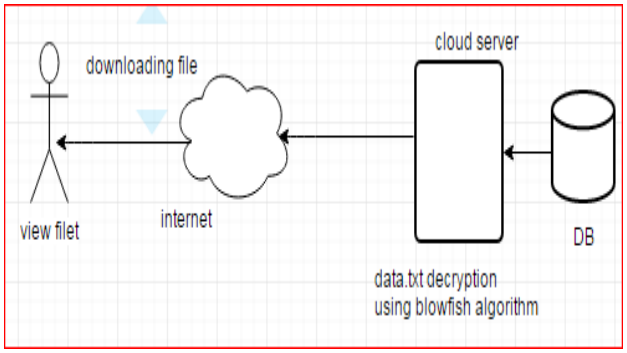

Fig. 5 Downloading Phase

Proposed systems with digital signature. Sender encrypted message using receiver public key with hash function. Add digital signature on encrypted data and send data to receiver. Receiver side decrypted message with sender`s private key.

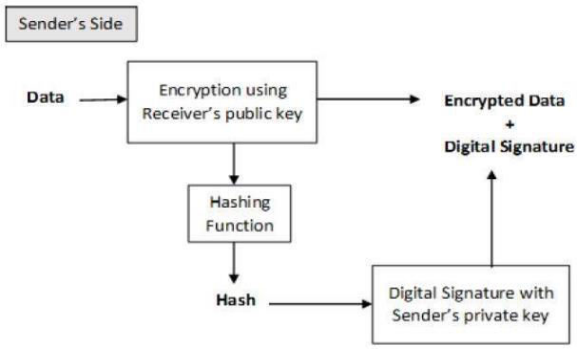

Fig. 5 Proposed Systems with Digital Signature

III Analysis

Proposed system implemented on open-shift public cloud. First, we create account on open shift and configure public cloud with following configurations

- JBoss Application Server
- MY SQL Server
- PHP MY Admin

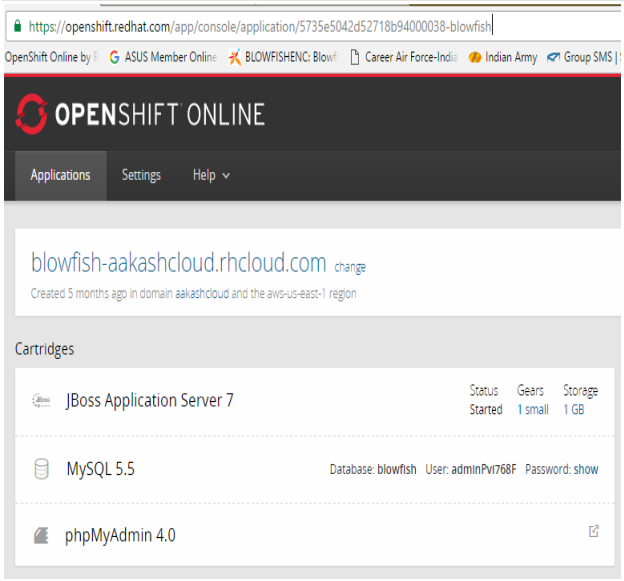

Fig. 6 Dashboard of public cloud

Table 1 File uploading and downloading Time Comparison

File ID	*File Name*	*File Size (Byte)*	*Uploading Time(ms)*	*Downloading Time (ms)*
F101	blowfish_db.sql	2797	5334.0	33.0
F102	viewUsers.java	707	1492.0	21.0
F103	ID aakash.docx	9967	18312.0	154.0

In public cloud user can upload and download file. At the time of uploading calculate hash value of file using SHA and encrypt file using Modified Blowfish algorithm. Here we calculate encryption and uploading time of file. When user downloads file then decrypt file using Modified Blowfish algorithm and calculate hash value of file. At this time, we calculate decryption and downloading time of file.

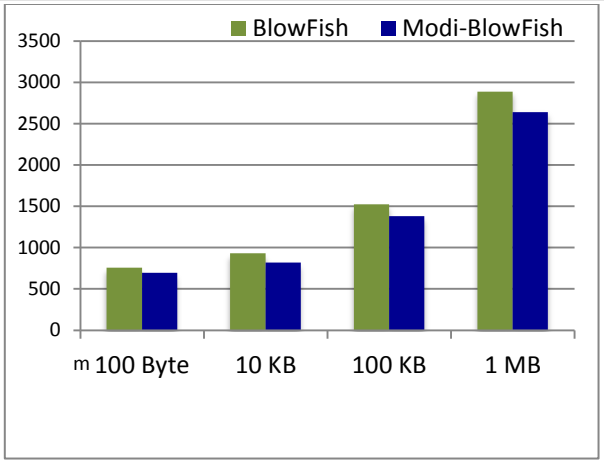

Fig. 6 Encryption Time of Different Size of Files

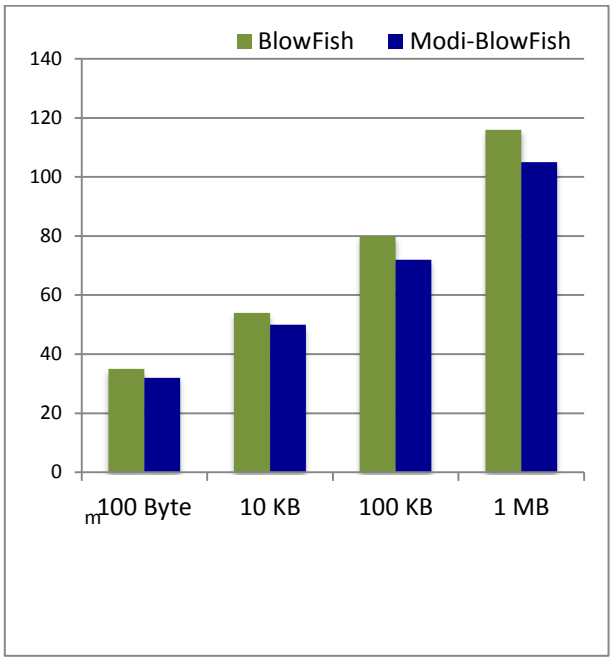

Fig. 7 Decryption Time of Different Size of Files

IV Conclusions

According to service delivery models and deployment models of cloud, data security and privacy protection are the primary problems that need to be solved. Data Security and privacy issues exist in all levels in SPI service delivery models. The above mentioned model is fruitful in data as a service, which can be extended in o their service models of cloud. Also it is tested in cloud environment like Open Shift, in future this can be deployed in other cloud environments and the best among of all can be chosen.

References

[1] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing", NIST, 2010.

[2] AkhilBehl, "Emerging Security Challenges in Cloud Computing", in Proc. of World Congress on Information and communication Technologies ,pp. 217-222, Dec. 2011.

[3] Srinivasarao D et al., "Analyzing the Superlative symmetric Cryptosystem Encryption Algorithm", Journal of Global Research in Computer Science, vol. 7, Jul. 2011.

[4] TingyuanNie and Teng Zhang "A study of DES and Blowfish encryption algorithm", in Proc. IEEE Region 10 Conference, pp. 1-4 ,Jan. 2009.

[5] Jitendra Singh Yadav et al.," Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" , International Journal of Advanced Research in Computer Science and Software Engineering ,vol. 2,Aug. 2012.

[6] Manikandan.Get al., "A modifiedcryptographic scheme enhancing data", Journal of Theoretical and Applied Information Technology, vol. 35, no.2, Jan. 2012.

[7] NileshMangtani and SukhadaBhingarkar, " The appraisal and Judgment of Nimbus, OpenNebula and Eucalyptus", International Journal of Computational Biology , vol. 3, issue 1, pp 44-47, 2012.

[8] A. Juels and B. S. Kaliski, Jr., (2007) ―Pors: proofs of retrievability for large files," in CCS '07: Proceedings of the 14th ACM conference on Computer and Communications security. New York, NY, USA: ACM, 584–597.

[9] Cody, Brian; Madigan, Justin; MacDonald, Spencer; Hsu, Kenneth W.;, "High speed SOC design for blowfish cryptographic algorithm," Very Large Scale Integration, 2007. VLSI SoC 2007. IFIP International Conference on , vol., no., pp.284-287, 15-17 Oct. 2007.

[10] Govinda.K1 Mythili and GeethaPriya(2014),‖ Data Security in Cloud using Blowfish Algorithm‖, International Journal for Scientific Research & Development| Vol. 2, Issue 09.

[11] J. Guo, S. Ling, C. Rechberger, and H. Wang, ―Advanced Meetin-the-Middle Preimage Attacks: First Results on Full Tiger, and Improved Results on MD4 and SHA-2,‖ pp. 1–20.

[12] GurpreetKaur and Manish Mahajan (2013), ―Analyzing Data Security for Cloud Computing Using Cryptography Algorithms‖, International Journal Of Engineering Research and Application, Vol.-3,782-786.