Achieve Confidentiality and Authentication for Cloud Computing Using Hybrid Approach

Nikita Khusbhoopawar

1Research Scholar 2Assistant Professor

1,2Department of Computer Science & Engineering
1,2Mahakal Institute of Technology Ujjain, M.P, India

Abstract—The security requirements for cloud computing providers begins with the same techniques and tools as for traditional data centers, which includes the application of a strong network security perimeter. Cloud computing servers use the same operating systems, enterprise and web applications as localized virtual machines and physical servers. Therefore, an attacker can remotely exploit vulnerabilities in these systems and applications. For security we apply blowfish algorithm on cloud store data. We also Modified blowfish algorithm and compare proposed algorithm with existing algorithm with different parameters like time and encryption time, decryption time, uploading and downloading time.

Key words: Encryption, Storage, Security, Blowfish algorithm

I. INTRODUCTION

Cloud computing can be defined as a new style of computing in which dynamically scalable and often virtualized resources are provided as a service over the internet. Cloud computing has become a significant technology trend, and many experts expect that cloud computing will reshape information technology (IT) processes and the IT marketplace. With the cloud computing technology, users use a variety of devices, including PCs, Laptops, smart phones, and PDAs to access programs, storage and application – development platforms over the Internet, via services offered by cloud computing providers. Advantage of cloud computing technology includes cost saving, high availability and easy scalability.

Cloud computing can be viewed as a collection of services, which can be presented as a layered cloud computing architecture, as shown in fig1. The services offered through cloud computing usually include IT services referred as to SaaS (Software-as-a-Service) which is shown on top of the stack. SaaS allows users to run applications remotely from the cloud. Infrastructure-as-a-Service (IaaS) refers to computing resources as a service. This includes virtualized computers with guaranteed processing power and reserved bandwidth for storage and Internet access. The data-Storage-as-a-service (dSaaS) provides storage that the consumer is used including bandwidth requirements for the storage.

Fig. 1: Layered architecture of cloud computing.

II. RELATED WORK

Privacy-Preserving Public Auditing for Secure Cloud Storage Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable [9] computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources [7].

N. Saravanan et. al. presents An Implementation of RSA Algorithm in Google Cloud using Cloud SQL. Cloud storage concern the user does not have control over data until he has been gain access. To provide control over data in the cloud data-centric security is needed. Before accessing the data it should satisfy the policy rules already defined. So cloud should enforce this scheme by using cryptographic approaches. We utilize RSA algorithm and Google App Engine to provide efficient and secured data storage scheme.

Shobha Rajak et. al. proposed a model for the integrity check over the cloud computing and we utilize the TPA and digital signature to achieve the integrity concept, in such a way to help the user to verify and examine the data from unauthorized people that manipulate with the cloud or extract from the data. Moreover, we are able to evaluate our work using a windows azure project that involves digital signature coding. As results, we found that our model worked well according to our claims. In future it can be enhancing in the server side updating and data modification. In our paper we decided to concern about the client data storing service in the cloud.[12].

Padmapriya et. al. presents[11] In Cloud computing technology there are a set of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability among others. But the most important between them is security and how cloud provider assures it. This paper analyses the importance of security to cloud. We compared three algorithms namely Data Encryption Standard (DES), RSA, Homomorphic encryption for data security in cloud. They are compared based on four characters; key used scalability, security applied to, and authentication type. In future we are going to propose a backup plan to solve security issues in both cloud providers and cloud consumers [14].

III. BLOWFISH ALGORITHM

Blowfish Algorithm created by Bruce Scherer in 1993. this algorithm is faster than AES, DES and triple DES.
Blowfish encryption algorithm is symmetric algorithm with following parameters

- **Simple**: It uses addition, XOR, lookup table with 32-bit operands.
- **Compact**: It runs in very less memory compared to other.
- **Fast**: It encrypts data on large 32-bit microprocessors at a rate of 26 clock/byte.
- **Secure**: More secure due to its key length from 32 to 448 bits. Default key length 128 bits.

Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time, it will follow the Feistel network and this algorithm is divided into two parts.

### A. Key-Expansion

Blowfish uses a big number of sub keys. These keys must be recomputed before any data encryption or decryption. The P-array consists of 18 32-bit subkeys: P_1, P_2, P_18. There are four 32-bit S-boxes with 256 entries each:

* The p-array consists of 18, 32-bit subkeys:
  * P_1, P_2, ..., P_18
* Four 32-bit S-boxes with 256 entries each:
  * S_1, S_1, 1, ..., S_1, 255
  * S_2, S_2, 1, ..., S_2, 255
  * S_3, S_3, 1, ..., S_3, 255
  * S_4, S_4, 1, ..., S_4, 255

### B. Data Encryption

It is having a function to iterate 16 times of network. Each round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 64-bit words. The only additional operations are four indexed array data lookup tables for each round. Pseudo code of blowfish is described below.

**IV. PROPOSED WORK**

This research proposes the latest improvement to the Blowfish formula. The proposed improvement uses the new operation defined in the previous section, operation ‘#’ applied during each round from the original Blowfish algorithm, where another key is needed to apply this operation at both sides, this key will come in binary form and convert to some 4-states key, or it may already also come in a 4-states as that you can do with quantum channel.

Therefore, two keys will double in each round from the original Blowfish, the first key K_1 will double with the X_L and P_i to generate the next left component. The second key K_2 will likely be used with F(X_L) and X_R to generate the right part. These three inputs on the ‘#’ operation should become firstly converted from 32 bits to some 16 digits each could possibly be one of four expresses (0, 1, 2, 3), when i.e., each two bits converted to its equivalent decimal numbers. Pseudo code of modify blowfish is described below.

![Fig. 2: Existing BlowFish Feistel Network.](image)

![Fig. 3: Modified Blowfish Feistel Network.](image)
V. IMPLEMENTATION AND RESULTS

Modified blowfish algorithm applies for encryption and decryption and compare proposed algorithm with existing algorithm with different parameters like time and encryption time, decryption time, uploading and downloading time. Proposed System is implement with the help of Openshift (RED-HAT) cloud using Openshift cloud we create public cloud with different tools like JBoss Server(Application Server), MySQL 5.5 (DATABASE), phpMyAdmin, Eclipse-Mars (IDE). We create user who can upload and download from cloud server. When user uploads file, firstly we encrypt the file using existing and modified blowfish algorithm and calculate time required for encryption in both algorithms. User downloads the file this time perform decryption using blowfish and modified blowfish algorithm and calculate decryption time. Encryption and decryption time is shown in figure 5 and 6.

![Encryption Time Chart](image1)

**Fig. 5: Encryption Time.**

![Decryption Time Chart](image2)

**Fig. 6: Decryption Time.**

VI. CONCLUSION

Traditional symmetric and asymmetric encryption schemes can be leveraged to provide Alice with a secure means through which she can send her message. However, with symmetric schemes each recipient will be in a position to decrypt all cipher-texts that have been encrypted with the same key: Access is too coarse-grained. With asymmetric schemes the encrypting entity needs to explicitly state for whom decryption is permissible: Access is too fine-grained. To reference the different styles of communication, symmetric schemes represent broadcast communication and asymmetric schemes unicast communication. The above Blowfish algorithm with AES in positions of the throughput,
Achieve Confidentiality and Authentication for Cloud Computing Using Hybrid Approach

 processing time. More the throughput, more the speed of the algorithm & less will be the power consumption. Finally we can conclude that Blowfish is the best of all. In future work we can perform Hardware Implementation to compare different parameters. This method is used for faster work. Implementations of Blowfish that require the fastest speeds should unroll the loop and ensure that all sub keys are stored in cache.

REFERENCES


