Improvising Information Security in Cloud Computing Environment

Shweta Sharma
Department of Computer Engineering
Delhi Technological University, India

Bharat Bhushan
STMicroelectronics India Pvt Ltd.
Greater Noida, India

Shalini Sharma
Department of Computer Engineering
Delhi Technological University, India

ABSTRACT
The evolution of internet has introduced an immense change in the usage of information and communication technologies. The fast, easy-to-use and pay per usage criteria leads to cloud computing infrastructure. Cloud Computing provides network services to its clients as per their requirements. Nowadays, information security has become a serious issue while client-server interaction in cloud computing environment. The privacy and integrity of information to be exchanged or stored needs to be protected to ensure a safe cloud computing platform establishment. In this paper, a security framework has been proposed to alleviate the security level of information transferred from client end to cloud service provider (server). Certain authentication and file integrity techniques have been studied and are suggested to be implemented under the proposed scheme. This way, scheme ensures good quality of confidentiality, Integrity and Authentication during storage and access of information in cloud computing. Certain cryptographic (symmetric and asymmetric) techniques have been used to design the proposed framework.

General Terms
Cloud computing, Security.

Keywords
Information security, integrity, authentication, cryptography, framework

1. INTRODUCTION
According to National Institute of Standards and Technology in the U.S. department of Commerce, cloud computing means:

'A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources(e.g. Networks, servers, storage applications etc.) that can be rapidly provisioned and released with minimal management effort or cloud provider (i.e., Internet Service Provider) interaction'[1].

There arise various scenarios where client would share confidential and sensitive information with the cloud service provider (such as transmission of credit card credentials or any other banking transactions) and in turn would expect certain level of privacy and security to avoid any kind of thwart attacks[2]. In this case, cloud server is completely responsible for safety and protection of client information until its retrieval[3]. Nowadays, a hacker being proactively engaged in performing certain kinds of security attacks[4] related to information confidentiality, integrity and authentication and hence, makes the job of cloud service provider more challenging and immediate to win the trust of its clients and makes cloud computing an effective solution[5].

As per [6], cloud computing faces around 10% data security issues which involves sensitive data, data loss, data integrity, redundancy etc. and so there arises a requirement to design a more secure framework to minimize such issues[7]. In the following paper, a scheme has been suggested to enable proper authentication, integrity establishment and confidentiality sustenance in cloud computing.

In given study, an Identity based authentication method is found suitable for cloud computing scenario .This ensures validity and identification of exact client during log-in interval .Cloud server authenticates client [8], thereby provides an accurate start for further client-server interaction. In this paper, an Identity based hierarchical model(IBHMCC) has been included which distinguishes each entity uniquely in a cloud .It involves Identity based encryption, decryption and corresponding signature schemes and an Identity based authentication (IBACC) as well[8].

It has been shown that IBACC has lightweight user side , efficient and provides large scalability to cloud systems. Hence this model proves to be a valid choice for proper authentication during client-server interaction in cloud computing systems.It has been shown that IBACC has lightweight user side , efficient and provides large scalability to cloud systems. Hence this model proves to be a valid choice for proper authentication during client-server interaction in cloud computing systems.

In order to provide file integrity, a light weight tool has been proposed which protects the user's file information while it resides on cloud server[9].It checks the file integrity by applying hash algorithm(such as MD5) and produces cryptographic checksum of the file information and subsequently stores on cloud. To verify established integrity, whenever the client asks for its already stored file, cloud server reapplies the same computation method and regenerates cryptographic checksum and matches with already stored one. If it's the same, it indicates there had been no outside security attacks on the stored file else integrity not established .The another advantage of this method is low memory usage as checksum value is stored within the file itself everytime after computation[9].

In given research work,a security framework has been designed for cloud computing in order to fulfill confidentiality, integrity and authentication criterias using symmetric and asymmetric cryptographic algorithms [10]. But there are certain problem areas in this work. Few issues have been shortlisted as follows:

- No valid authentication scheme had been proposed or implemented.

- Server storage security criteria had not been considered while client-server interaction.
- Weak and less secure framework (as concatenations are more vulnerable to brute-force attacks).
- Randomness related security factors had been ignored completely.
- This framework can't be preferred for highly confidential data (related to banking, defense and other brokerage related applications).

The rest of the paper is organized as follows: Section 2 provides the design of proposed security scheme including framework to increase information security. Section 3 explains the cryptographic algorithms used to design the proposed framework. Section 4 includes conclusion of this research work.

2. PROPOSED SCHEME

A security scheme for client-server interaction in cloud computing has been proposed here .It includes following techniques:

- Identity Based Authentication.
- Server file storage integrity concept.
- Proposed security framework.

Following are the sequence of events to be executed under this scheme:

- Client-Server Authentication occurs on the machine using Identity Based algorithm for authentication purpose [8].
- After valid authentication, client requests server to store his/her file.
- Server stores the respective file on its hard disk and generate a keyed hash value for file (using SHA-1 and encryption algorithm)[9].
- Whenever client requires its data back, it sends a request to server to resend the respective file.
- Server checks for the file integrity (by recalculating the hash value for the file and matches with originally stored hash value. If values match, it signifies file is intact otherwise has been modified by any outside intruder).
- After integrity establishment, server decrypts the file and encrypts again using the proposed framework of symmetric and asymmetric algorithms for secure and confidential transfer of data from server to client[11,12].
- Session key is generated and shared through server for every new created session b/w client and server.

The architecture of proposed security scheme is illustrated in Fig. 1 .

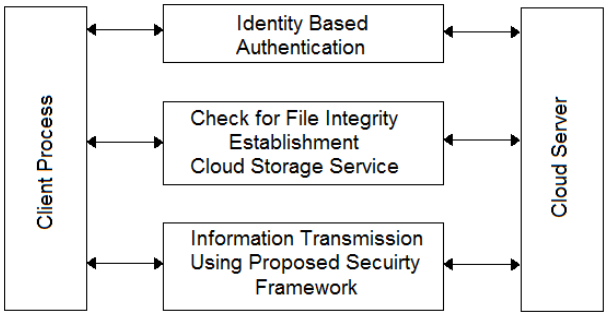

Fig 1: The architecture of proposed security framework

The proposed security framework diagram is shown in Fig.2.

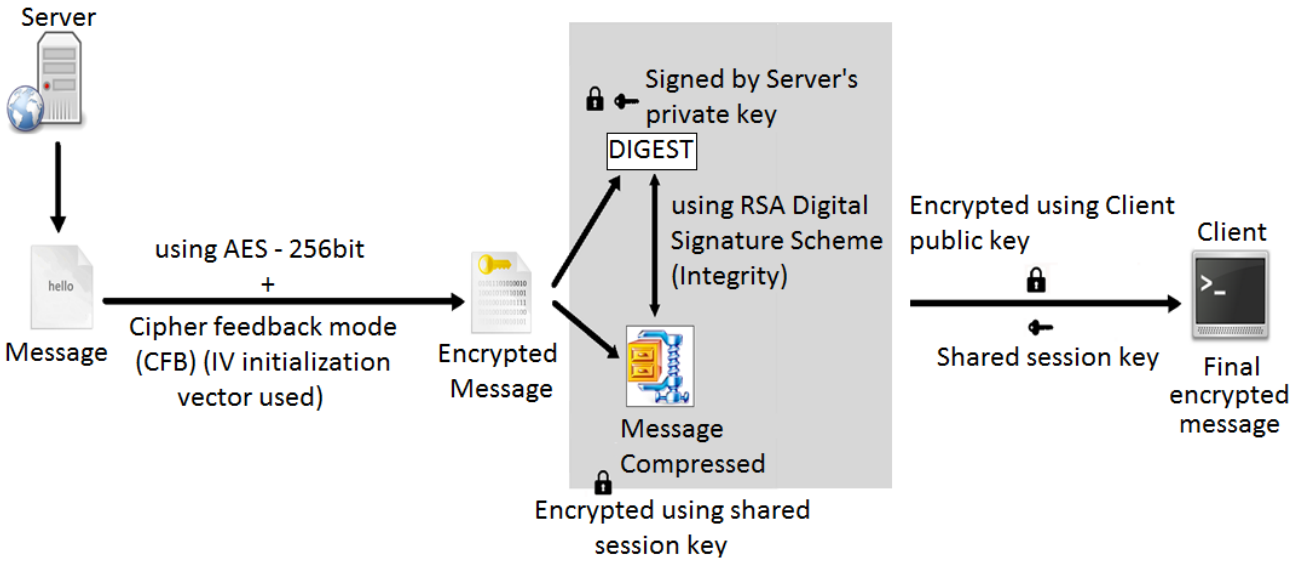

Fig 2: Proposed Security Framework

The features of above proposed security scheme are listed as follows:

- It provides secure storage on server for client's data (Integrity establishment) using RSA digital Signature scheme.
- AES-256 bit key encryption (for confidentiality purpose).
- SHA-512/HMAC to generate digest (enhances security and integrity).
- ZIP algorithm (compression algorithm) to reduce traffic flow between client and server (optional).
- Double encryption and cyclic codes are introduced to increase randomness in the ciphertext.
- Shared Session Key acts as an extra layer of security for this model.

- Timestamp is also considered to be incorporated in the proposed model.
- This model meets the standard requirements for data security [13](includes confidentiality, Data Integrity, Authentication) as desired.
- This framework enhances the level of security which can be achieved for information transmission.

3. ALGORITHMS USED

3.1 AES-256 (Advanced Encryption Standard)

The advanced encryption standard is a symmetric-key block cipher published by National Institute of Standards and Technology NIST).AES-256 is a non feistal cipher that encrypts and decrypts a data block of 128 bits. It uses 14 rounds and keysize is 256 bits[14].

The general design of AES encryption cipher is shown in Fig.3.

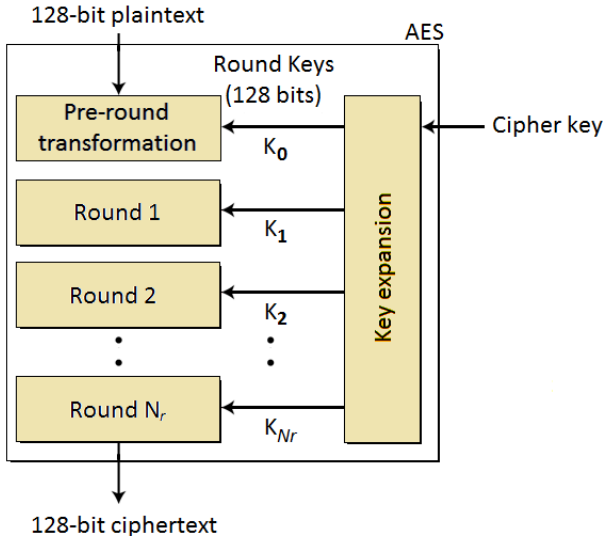

Fig 3: General design of AES Encryption

3.2 Cipher Feedback Mode (CBC)

This technique assists in producing randomness to the cipher text sequence generated through AES-256 as mentioned in proposed security framework. The k-bit cipher feedback mode is shown in Fig.4.

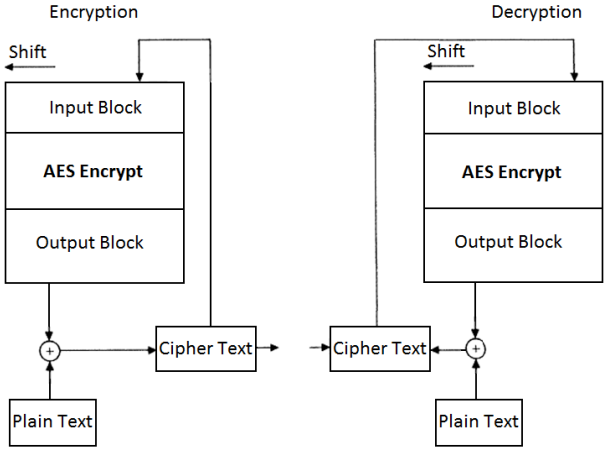

Fig 4: K-bit Cipher Feedback Mode (CBC)

3.3 RSA Digital Signature Scheme

Under this scheme, digital signature is established using RSA (Asymmetric algorithm).Here, d is private and e , n are public .The key generation process of this scheme resembles the key generation process in RSA itself.

In this case, the signature (S) produced by signer is verified using (e, n) and if M'=M, then it indicates digital signature scheme has been setup and verified as well.

In proposed framework, this digital signature scheme has been used to establish integrity and enhancement of security levels between client and server during transmission of confidential information.

The concept of RSA Digital Signature is shown in Fig.5

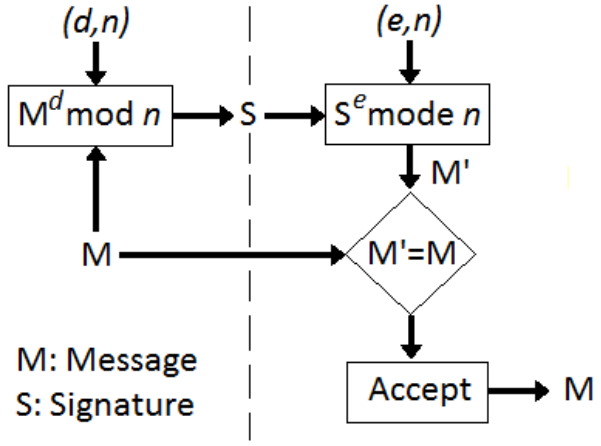

Fig 5: RSA Digital Signature Scheme

3.4 ZIP Algorithm

This algorithm is a data compression algorithm and has been applied in framework to minimize the size of encrypted information to be sent to the client end.It decreases the effective network payload during information communication.

4. CONCLUSION

In order to sustain the confidentiality of client data, this security scheme has been designed. This way, a desirable amount of security can be provided during information exchange between client and cloud (server). This proposal can be implemented in a cloud computing infrastructure and proves to be cost effective and alleviates security level in cloud and thus establishes the trust between both the parties for further business prospects. For future enhancements, various security threats scenarios can be analyzed and their security solutions can be proposed and simulated effectively.

5. REFERENCES

[1] G A Solanki, "Welcome To The Future of Computing: Cloud Computing And Legal Issues ",International journal of scientific and technology , vol.1, no.4, pp., Oct 2012.

[2] Lijun Mei, W.K.Chan, T.H.Tse, "A Tale of Clouds: Paradigm comparisons and some thoughts on research issues", 2008 IEEE Asia-Pacific Services Computing Conference.

[3] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono, "On technical security issues in cloud computing" 2009, IEEE Computer Society.

[4] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr.Atanu Rakshit, "Cloud security Issues"2009, IEEE.

[5] Guy Bunker, Farnam Jahanian, Aad van Moorsel, Joseph Weinman,"Dependability in the cloud: Challenges and opportunities", IEEE 2009.

[6] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund, Makan Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud computing", Gonzalez et al. Journal of Cloud Computing: Advances, Systems and Applications2012,http://www.journalofcloudcomputing.com/content/1/1/11.

[7] John Harauz, Lori M. Kaufman, Bruce Potter, "Data security in the world of cloud computing",2009 IEEE CO Published by the IEEE Computer and Reliability Societies.

[8] Hongwei Li, Yuanshun Dai, Ling Tian and Haomiao Yang, "Identity-Based Authentication for Cloud Computing", Springer-Verlag Berlin Heidelberg 2009.

[9] Sanchika Gupta, Anjali Sardana, Padam Kumar, "A light Weight Centralized File Monitoring Approach for Securing Files in Cloud Environment ", The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012) ©IEEE 2012.

[10] M.Sudha, M.Monika, "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography", Advances in Computer Science and its Applications 32 Vol. 1, No. 1, March 2012, Copyright © World Science Publisher, United States. www.worldsciencepublisher.org

[11] A secure and light weight approach for critical data security in cloud : 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN).

[12] Siani Pearson" Taking account of Privacy when Designing Cloud computing Services CLOUD'09, May 23, 2009, Vancouver, Canada ,2009 IEEE.

[13] Cong Wang, Qian Wang and Kui Ren,"Ensuring Data Storage Security in Cloud computing"978-1- 4244 - 3876-1/2009 IEEE

[14] Forouzan, "Cryptography and Network Security", TMH 2012.