International Journal of Research Studies in Science, Engineering and Technology
Volume 1, Issue 9, December 2014, PP 103-109
ISSN 2349-4751 (Print) & ISSN 2349-476X (Online)

The Security of Cloud Computing System Enabled by Shamir's Secret Sharing Algorithm

M. Padmavathi*, D. Sirisha[#], A. LakshmanRao[#]

*M.Tech from Pragati Engineering College, JNTU Kakinada, A.P.
[#]Faculty for Computer Science at Pragati Engineering College, JNTU Kakinada, A.P.

Abstract: *Distributed computing principally assigns numerous clients and extremely adapting method for exchanging the information through the system. High potentials of distributed computing can be exploited with the gathering of individuals with little range of office and others. In such computing environments security issues may crop up and affect the clients who are associated in a system. To ensure security locally trusted figuring stage is utilized efficiently. In the present work a novel security algorithm Shamir's mystery imparting calculation in the distributed environment is proposed.*

Keywords: *Security in Cloud Computing, Trusted Computing, Shamir's Secret Sharing algorithm.*

1. INTRODUCTION

Cloud computing is an environment that includes a large number of computers associated through a communication network such as the Internet [4]. Cloud computing is a synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time. Network-based services, which appear to be delivered by real server hardware and are in fact served up by virtual hardware simulated by software running on one or more real machines, is often called cloud computing. Such simulated servers do not physically exist and can therefore be relocated around and scaled up or down on the fly without disturbing the end user, somewhat like a cloud becoming larger or smaller without being a physical object [3].

The major models of cloud computing service are known as software as a service, platform as a service, and infrastructure as a service [3].Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network [6]. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. The cloud also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users.

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of virtualization [4] [7]. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures [8]. An alternative perspective on the topic of cloud security is that this is but another, although quite broad, case of "applied security" and that similar security principles that apply in shared multi-user mainframe security models apply with cloud security [9].

Cloud computing offers many benefits, but is vulnerable to threats. As cloud computing uses ways to exploit system vulnerabilities. Underlying challenges and risks in cloud computing increase the threat of data compromise. To mitigate the threat, cloud computing stakeholders should invest heavily in risk assessment to ensure that the system encrypts to protect data, establishes trusted foundation to secure the platform and infrastructure, and builds higher assurance into auditing to strengthen compliance. Security concerns must be addressed to maintain trust in cloud computing technology.

2. THE SECURITY ALGORITHMS

Security in cloud is one of the major areas of research. Researchers are focusing on efficient algorithms and cryptography techniques to enhance the security in cloud computing.

Broadly, Cryptographic systems provide us three types of cryptographic algorithms namely, Secret Key Cryptography (SKC), Public Key Cryptography (PKC) and Hash Functions.

The Secret Key Cryptography (SKC) uses a single (same) key for the process of encryption and decryption.

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people.

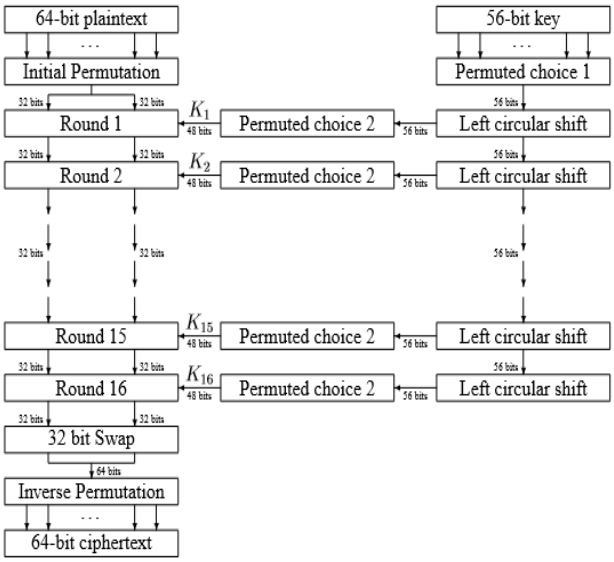
Decryption is the process of converting encrypted data back into its original form, so it can be understood.

The well known SKC algorithms are:

2.1 Data Encryption Standard (DES)

DES was designed in 1970's by IBM and was ratified in 1977 by the National Bureau of Standards (NBS) for commercial use. It is a block cipher that operates on 64-bit blocks employing a 56-bit key and 8 rounds. Although DES has been around long back but no real weakness has been identified. The biggest disadvantage of DES is the 56 bit key size.

A DES key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte.



Overall structure of DES Algorithm

2.2 Advanced Encryption Standard (AES)

AES was designed by Vincent Rijmen and Joan Daemen and was introduced in 1998. The algorithm can use fickle key length and block length. The key length can include 128, 192, or 256 bits and block length can be of 128, 192, or 256 bits.AES is a highly efficient and secure algorithm. The drawback lies in its processing as it requires more processing.

The input and output for the AES algorithm each consist of sequences of 128 bits (digits with values of 0 or 1). These sequences will sometimes be referred to as blocks and the number of bits they contain will be referred to as their length. The Cipher Key for the AES algorithm is a sequence of 128, 192 or 256 bits. Other input, output and Cipher Key lengths are not permitted by this standard. The bits within such sequences will be numbered starting at zero and ending at one less than the sequence length (block length or key length). The number i attached to a bit is known as its index and will be in one of the ranges $0 \le i < 128$, $0 \le i < 192$ or $0 \le i < 256$ depending on the block length and key length.

All byte values in the AES algorithm will be presented as the concatenation of its individual bit values (0 or 1) between braces in the order {b7, b6, b5, b4, b3, b2, b1, b0}

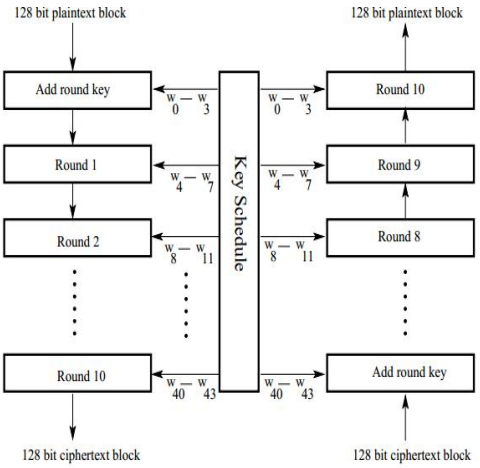
$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 = \sum_{i=0} b_i x^i$

The basic unit for processing in the AES algorithm is a byte, a sequence of eight bits treated as a single entity. For an input, output or Cipher Key denoted by a, the bytes in the resulting array will be referenced using one of the two forms, an or a[n], where n will be in one of the following ranges:

Key length = 128 bits, $0 \leq n < 16$; Block length = 128 bits, $0 \leq n < 16$;

Key length = 192 bits, $0 \leq n < 24$;

Key length = 256 bits, $0 \leq n < 32$.



The overall structure of AES algorithm for the case of 128-bits

2.3 Rivest Cipher (RC)

Ronald Rivest developed this algorithm and thus, the name of the algorithm was put after Ronald's Rivest name. It provides a series of RC algorithms including RC1, RC2, RC3, RC4, RC5 and RC6.

- RC1 was never published.
- RC2 was a 64-bit block cipher developed in 1987.
- RC3 was broken before ever being used.
- RC4 is the world's most widely used stream cipher.
- RC5 is a 32/64/128-bit block cipher developed in 1994.
- RC6, a 128-bit block cipher based heavily on RC5, was an AES finalist developed in 1997.

2.4 Blowfish

Blowfish was developed by Bruce Schneie and was first published in the year 1993. This block cipher has 8 rounds, having the block size is of 64 bits and the key length can vary from 32 to 448 bits. Blowfish was proposed as a substitute was DES. This algorithm is significantly faster than other algorithms and the key strength is excellent. Blowfish algorithm is apt only for applications where the key mostly remains the same.

Blowfish uses large number of sub keys. These keys are generating earlier to any data encryption or decryption.

The p-array consists of 18, 32-bit sub keys:

P1, P2…P18

Four 32-bit S-Boxes consist of 256 entries each:

S1, 0, S1, 1… S1, 255

S2, 0, S2, 1… S2, 255

S3, 0, S3, 1… S3, 255

S4, 0, S4, 1… S4, 255

The Public Key Cryptography (PKC) uses one (public) key for encryption and another (private) key for decryption.

The PKC algorithms that are used now-a-days are:

2.5 RSA

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman. RSA was named after the mathematicians who invented it. RSA was first published in 1997. Variable size key and encryption block is used in RSA. Main advantage of RSA algorithm is enhanced security and convenience. Using Public Key Encryption is also an advantage of this algorithm. RSA lacks in encryption speed.

2.6 Diffie-Hellman

Diffie-Hellman algorithm was introduced in1976 by Diffie-Hellman. The Diffie-Hellman algorithm grants two users to establish a shared secret key and to communicate over an insecure communication channel. One way authentication is free with this type of algorithm. The biggest limitation of this kind of algorithm is communication made using this algorithm is itself vulnerable to man in the middle attack.

2.7 ElGamal Algorithm

ElGamal algorithm was developed in the year 1984 by Taher Elgamal. It is an asymmetric key algorithm and is based on Diffie-Hellman key exchange. ElGamal encryption can be described over any cyclic group G. The security relies upon the issue of a problem in G related to computing discrete logarithms. Fast generalized encryption for long messages and data expansion rate are the two biggest advantages of this algorithm. The chief drawback of ElGamal is the requirement for randomness and its slower speed.

Hash Functions, also known as message digest, are the algorithms that do not use any key. Based upon the plain text, a fixed length hash value is generated.

Message Digest (MD) algorithm

It produces a hash value of 128 bit from an arbitrary length message. The MD series includes MD2, MD4 and MD5.

2.8 MD5 Algorithm

The MD5 algorithm was developed by Rivest in 1991 and is an extension of the MD4 message-digest algorithm and is bit slower than MD4. This algorithm results in a 128 bit hash value. It is mostly used in security based applications. MD5 is more secure than MD4. It is suitable to use for standard file verifications but it has some flaws and therefore, it is not useful for advanced encryption applications.

As stated earlier that the main purpose of this paper is to study the use of cryptographic algorithms in the field of cloud computing and to provide navigation to the naive users. The searches were checked and examined several times to find their appropriate areas. The PKC algorithm in this paper is.

Adi Shamir stated the unique definition for trust in cloud computing and various issues related to security are discussed here. Shamir's secret sharing algorithm calculates the security rate very efficiently and execution time is faster in cloud computing environment.

Jensen M. stated that The Cloud Computing concept offers dynamically scalable resources provisioned as a service over the Internet. Economic benefits are the main driver for the Cloud, since it promises the reduction of capital expenditure (CapEx) and operational expenditure (OpEx). In order for this to become reality, however, there are still some challenges to be solved. Amongst these are security and trust issues, since the user's data has to be released to the Cloud and thus leaves the protection-sphere of the data owner. Most of the discussions on these topics are mainly driven by arguments related to organizational means. This paper focuses on technical security issues arising from the usage of Cloud services and especially by the underlying technologies used to build these cross-domain Internet-connected collaborations

3. EXISTING SYSTEM

Trusted cloud computing platform (TCCP) that provides a closed box execution environment by extending the concept of trusted platform to an entire IaaS backend. The TCCP guarantees the confidentiality and the integrity of a user's VM, and allows a user to determine up front whether or not the IaaS enforces these properties.

The model of trusted computing is originally designed to provide the privacy and trust in the personal platform and the trusted computing platform is the base of the trusted computing. Since the internet computing or network computing has been the main computing from the end of the last century, the model of trusted computing is being developed to the network computing, especially the distributed systems environment. The cloud computing is a promising distributed system model and will act as an important role in the e-business or research environments. As web service technology have developed quickly and have been used broadly, cloud computing system could evolve to cloud computing service, which integrates the cloud computing with web service technology. So we could extend the trusted computing mechanism to cloud computing service systems by integrating the TCP into cloud computing system.

In cloud computing environment, different entities can appeal to join the CLOUD. Then the first step is to prove their identities to the cloud computing system administration. Because cloud computing should involve a large amount of entities, such as users and resources from different sources, the authentication is important and complicated. Considering these, we use the TCP to aid to process the authentication in cloud computing.

The Trusted Computing Platform (TCP) is based on the Trusted Platform Module (TPM). The TPM is a logic independent hardware. It can resist the attack from software, and even the hardware attack. The TPM contain a private master key which can provide protect for other information store in cloud computing system. Because the hardware certificate can store in TPM, it is hard to attack it. So TPM can provide the trust root for users.

Since the users have full information about their identity, the cloud computing system can use some mechanism to trace the users and get their origin. Because in the TCP the user's identity is proved by user's personal key and this mechanism is integrated in the hardware, such as the BIOS and TPM, so it is very hard to the user to make deceiving for their identity information. Each site in the cloud computing system will record the visitor's information. So by using the TCP mechanism in cloud computing, the trace of participants can be known by the cloud computing trace mechanism.

4. THE PROPOSED SYSTEM

Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

Counting on all participants to combine together the secret might be impractical, and therefore sometimes the threshold scheme is used where any k of the parts are sufficient to reconstruct the original secret.

Mathematical definition

The goal is to divide secret S (e.g., a safe combination) into n pieces of data $D_1 \ldots D_n$ in such a way that:

1. Knowledge of any k or more D_i pieces makes S easily computable.

2. Knowledge of any k-1 or fewer D_i pieces leaves S completely undetermined (in the sense that all its possible values are equally likely).

This scheme is called \left (k,n\right) threshold scheme. If k=n then all participants are required to reconstruct the secret.

Shamir's secret-sharing scheme

The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes k\, \! Points to define a polynomial of degree k-1

Suppose we want to use a (k,n) threshold scheme to share our secret without loss of generality assumed to be an element in a finite field F of size P where 0 < k ≤ n < P; S<P and P is a prime number.

Choose at random k - 1 positive integers$a_1 \ldots a_{k-1}$ with a_i< P and let a0 = S. Build the polynomial

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots + a_{k-1} x^{k-1}$$

Let us construct any n points out of it, for instance set i = 1, ---, n to retrieve (i, f (i)). Every participant is given a point (an integer input to the polynomial, and the corresponding integer output). Given any subset of k of these pairs, we can find the coefficients of the polynomial using interpolation. The secret are the constant terma_0.

One Time Password

One Time Password (OTP) authentication is a method to reduce the potential for compromised user credentials. The concept behind OTP is that every session initiated by a user generates a unique user credential that is only valid for that session or for a very short period of time. Even if an attacker is capable of obtaining this user credential, it may either no longer be valid or be prohibited from additional use [12].

Security of one-time-password protocols

The main security property that protocols employing one-time passwords should achieve is: strong mutual authentication based on knowledge of one-time passwords. Our work will address one-time passwords in the context of PAKE protocols, which provide an additional property: secure key exchange.

The motivation for using one-time passwords is that the compromise of one password should not affect the security of sessions involving another password. The one-time password serves to mutually authenticate the client and the server; there are no other long-term values like public keys or certificates. Authentication is based on knowledge of the shared password. Informally, a protocol will provide secure mutual authentication if no honest party A^ accepts a session as being with party B^ unless B^ participated in the protocol, and vice versa. We want a one-time-password protocol to give secure mutual authentication for the current session even if other one-time passwords have been revealed [12].

In addition to mutually authenticating two parties to each other, we want a protocol that will also output session key that can be used to encrypt and protect the integrity of future communications between those two parties. This is a common feature required of many secure communication protocols. The traditional use of one-time passwords – sending the password over an SSL connection – is not compatible with our approach. Using SSL to establish an authentic channel requires that the user can obtain and properly use an authentic public key for the server. In other words, it requires a public key infrastructure, where as one-time-PAKE only needs shared passwords.

5. EXPERIMENTAL RESULTS

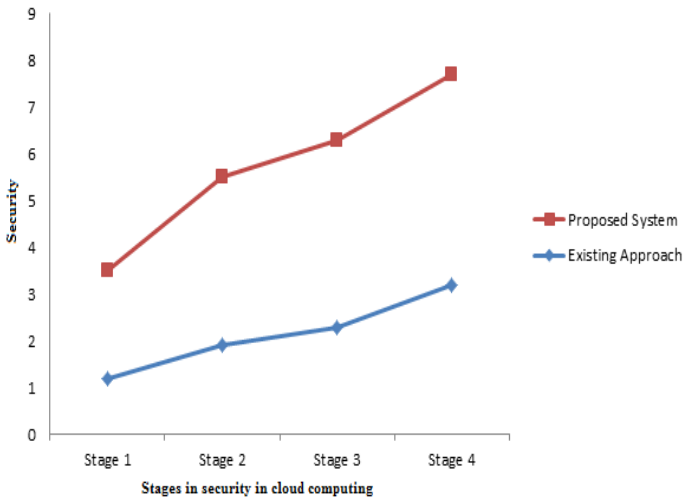


Fig No.1

In our results we mainly show that there is vast difference in security provided by existing approach and proposed system.

Graph showing the difference between two approaches

From the above graph it can be observed that our proposed approach has yielded high security when compared with native approach. The different stages are occurring in cloud computing are considered as the data from one system to other. It can also be observed that at each stage the proposed strategy obtained high security.

6. CONCLUSION

In this paper we conclude that in cloud computing the main important factor is security that will be the primary need of any user who are accessing in a particular network. The native approach which is trusted computing platform may not give maximum security to the users. In the present work, a new Shamir's secret sharing algorithm is proposed. The experimental study reveals that Shamir's secret sharing algorithm yields maximum security compared to the existing system.

REFERENCES

[1] " Cloud Computing and the Lessons from the Past ".Mikkilineni, Rao.

[2] "On Technical Security Issues in Cloud Computing ".Jensen, M.

[3] "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance". Tim Mather

[4] "Securing Virtual and Cloud Environments". In I. Ivanovo et al. Cloud Computing and Services Science, Service Science: Mariana Carroll, Paula Kotzé, Alta van der Merwe.

[5] "Cloud Computing entry". Net Lingo.

[6] "The NIST Definition of Cloud Computing". National Institute of Standards and Technology. Retrieved 24 July 2011.

[7] "Secure virtualization: benefits, risks and constraints, 1st International Conference on Cloud Computing and Services Science". M Carroll, P Kotzé, Alta van der Merwe (2011).

[8] "Addressing cloud computing security issues". Future Generation Computer Systems. Zissis, Dimitrios; Lekkas (2010).

[9] "Securing the Cloud: Cloud Computer Security Techniques and Tactics ". Waltham.

[10] "One Time Password Authentication for Open High Performance Computing Environments". Stephen Chan, Stephen Lau slau, Adrian Wong.

[11] "Towards Trusted Cloud Computing ". Nuno Santos Krishna P. Gummadi Rodrigo Rodrigues.