Data Security in Cloud Based on Trusted Computing Environment

Vijay .G.R, A.Rama Mohan Reddy

Abstract- ***In recent years Cloud Computing has become one of the growing fields in computer science. In which the security problem of cloud computing has become a hot research topic. It must be verified in the trusted status of the platform which actually carries out the computing task in the cloud, and the remote mechanism in Trusted Computing is suited for the cloud user's verification need.***

This paper briefly sketches out the method to build a Trusted Computing Environment for cloud computing system by integrating the Trusted Computing Platform (TCP) with Trusted Platform Module (TPM) into the security of cloud computing system. The RC4 stream cipher algorithm is most used algorithm to provide the confidentiality over the different networks. In this paper we propose the discussion of Simulation Results with its Analysis and the Performance Evaluation with the representation of data and time.

Keywords-- Cloud Computing, TCP, TCM, Trusted Computing, RC-4.

I. INTRODUCTION

Cloud computing is a promising computing paradigm which recently has drawn extensive attention from both in industry and academia. By combining a set of existing and new techniques from research areas such as Service-Oriented Architectures (SOA) and Virtualization, cloud computing is regarded as such a computing paradigm in which resources in the computing infrastructure are provided as services over the Internet. As promising as it is, cloud computing is also facing many challenges that, if not well resolved.

Data security is among these challenges that would raise great concerns from users when they store sensitive information on cloud servers.

These concerns originate from the fact that cloud servers are usually operated by commercial providers which are very likely to be outside of the trusted domain of the users.

The dependable and secure computing includes not only security and confidentiality, but also reliability, availability, safety and integrity. Considering these facts, proposed a new way that is conducive to improve the secure and dependable computing in cloud.

In our design, integrating the Trusted Computing Platform, which is based on Trusted Platform Module, into the cloud computing. The TCP will be used in authentication, confidentiality and integrity in cloud computing environment that will not bring much complexity to users. Because the TCP is based on relatively independent hardware modules, it does not cost too much resource of CPU, and can improve the performance of processing cryptographic computation system by using RC4 cipher algorithm. We also design a software as middleware, the Trusted Platform Support Service (TSS), on which the cloud computing application can use easily the security function of TPM.

II. DATA SECURITY IN CLOUD

A. Existing Method

In order to archive security in cloud computing system, some technologies have been used to build the security mechanism for cloud computing. Security messages and secured messages can be transported, understood, and manipulated by standard Web services tools and software. The cloud includes distributed users and resource from distributed local systems or organizes, which have different security policies. According to this reason, how to build a suitable relationship among them is a challenge. In fact, the requirements for the security in cloud computing environment have some aspects, including confidentiality, multiple security policy, and dynamic of the services. The Drawbacks in present using security methods are

a. There is short of the mechanism on the hardware to support the trusted computing in cloud computing system.

b. The trusted root in cloud computing environment has not been defined clearly. The creation and protection of certificates are not secure enough for cloud computing environments.

c. The performance is reduced apparently when the cryptographic computing are processed.

d. There are also lack of some mechanisms to register and classify the participants carefully, such as the tracing and monitoring for them.

B. Proposed Method

Cloud computing provides people the way to share distributed resources and services that belong to different organizations or sites. Since cloud computing share distributed resources via the network in the open environment, thus it makes security problems important for us to develop the cloud computing application. The main Solution to make secure for data or resources is,

a). Propose a method to build a trusted computing environment for cloud computing system by integrating the Trusted Computing Platform (TCP) into cloud computing system.

b). Propose a model system in which cloud computing system is combined with Trusted Computing Platform (TCP) with Trusted Platform Module (TPM). From which we can get some important security services, including authentication, confidentiality and integrity, in cloud computing system.

Manuscript received on March, 2013.

Vijay.G.R, PhD Scholar, Department of Computer Science & Engg, JNTUA, Anantapur, A.P, India.

Dr.A.Rama Mohan Reddy, Professor, Dept. of CSE, SVU College of Engineering, Tirupati, A.P, India.

III.TRUSTCOMPUTING ENVIRONMENT

The prominent approach to Trusted Computing Technology (TCP) has been specified by the Trusted Computing Group (TCG). The TCG proposes to extend common computing platforms with trusted components in software and hardware.

A.Trusted Computing Platform (TCP)

When the user login the cloud computing system, his identity information should be recorded and verified at first. Each site in the cloud computing system will record the visitor's information. So if the TCP mechanism is integrated into the cloud computing, the trace of the participants, including the users and other resources, can be knew by the cloud computing trace mechanism. Then if the participants do some malicious behavior, they will be tracked and be punished. In order to achieve the trusted computing in the cloud computing system should have the mechanism to know not only what the participants can do, but also what the participant have done. So the monitoring function should be integrated into the cloud computing system to supervise the participants' behavior. In fact, reference monitors have been used in the operation system for more than several decades, and it will be useful in cloud computing too.

B. Trusted Platform Module (TPM)

A Trusted Platform Module (TPM) has been defined as a logical bundle of functionality, together with a means to embed it in the PC architecture. The functional behavior of the TPM can be implemented wholly in software, but some of its behaviors such as the strong protection of a platform-specific unique secret key require protections which can be achieved only through a hardware device. To provide stronger computer security than software alone can provide, TCG has defined the specification for the widely implemented Trusted Platform Module. A Trusted Platform is a normal open computer platform that has been changed to achieve security. The main functionalities of this Trusted Platform are

-A mechanism for the platform to give that it's executing the expected software.

-To prove that it's a Trusted Platform while maintaining secrecy (if required).

-It will provide Protection against theft and misuse of secrets held on the platform.

IV. DESIGN

A. Input Design

The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy.

Input Design should consider about what type of data should be given as input? How the data should be arranged or coded? The dialog to guide the operating personnel in providing input and Methods for preparing input validations and steps to follow when error occur.

- Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
- It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
- When the data is entered it will check for its validity. Data can be entered with the help of screens. Thus the objective of input design is to create an input layout that is easy to follow.

B. Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs.

In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

- Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
- Select methods for presenting information.
- Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more objectives like, Convey information about past activities, current status or projections of the future, Signal important events, opportunities, problems, or warnings, Trigger an action and confirm an action.

C. Process Flow Chart

A flowchart is a type of diagram that represents an algorithm or process, showing the steps as boxes of various kinds, and their order by connecting these with arrows. This diagrammatic representation can give a step-by-step solution to a given problem. Process operations are represented in these boxes, and arrows connecting them represent flow of control. Data flows are not typically represented in a flowchart, in contrast with data flow diagrams rather, they are implied by the sequencing of operations.

Like other types of diagram, they help visualize what is going on and thereby help the viewer to understand a process, and perhaps also find flaws, bottlenecks, and other less-obvious features within it. The two most common types of boxes in a flowchart are:

- A processing step, usually called activity, and denoted as a rectangular box
- A decision usually denoted as a diamond.

D. Sequence Diagram

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called Event-trace diagrams, event scenarios, and timing diagrams. A sequence diagram shows, as parallel vertical lines ("lifelines"), different processes or objects that live simultaneously, and, as horizontal arrows, the messages exchanged between them, in the order in which they occur. This allows the specification of simple runtime scenarios in a graphical manner.

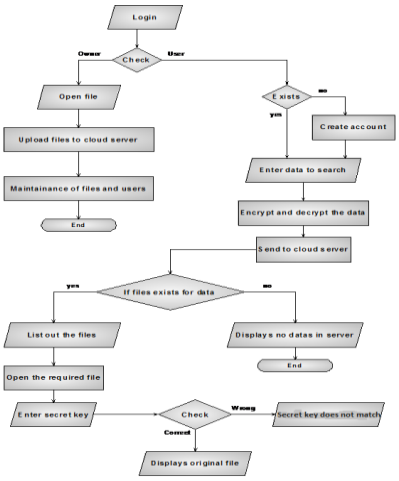

Figure 1. Process Flow Chart

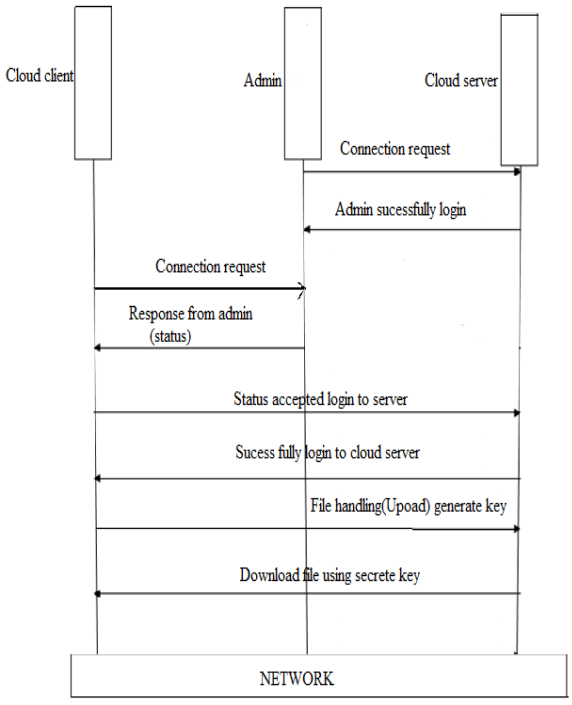

Figure 2. Sequence Diagram

Module Implementation will mainly consists of two modules

1). Client module: Has three GUI buttons to process information and access data from cloud server.
   a. Administrator: Administrate all the new user requests based on TCP technique.
   b. Client: Clients as users of cloud server.
   c. Create new user: This user interface button is used to create new users using username and password mechanism.

2). Cloud server module: This module contains two GUI buttons and one text box to display TCP view of particular client machine
   a. TCP view: Determines the TCP view of particular client machine.
   b. Stop server: Shut down cloud server.

V. RC4 CIPHER ALGORITHM

One of the most preferred stream cipher algorithm is Rivets's Cipher- 4(RC4) stream cipher algorithm. In this algorithm there are two stages process during encryption as well as decryption. The algorithm is dividing into the two parts KSA (Key scheduling Algorithm) and PRGA (Pseudo Random Generator Algorithm). KSA as the first stage of algorithm also knows as initialization of S (s is state vector) and PRGA known as stream generation in the RC4 whole process of algorithm. In the first stages of RC4 Stream Cipher algorithm on the bases of variable sized key from 1 to 256 or 0 to 255 a State Table of fixed length 256 bytes is generated, after we generate the key stream that XOR with plaintext and cipher text during encryption and decryption. During encryption the key stream is XOR with the plaintext and during decryption the cipher text XOR with key stream then convert into the plaintext.

A. The Key-Scheduling Algorithm (KSA)

The key-scheduling algorithm is used to initialize the permutation in the array "S". "Key Length" is defined as the number of bytes in the key and can be in the range $1 \leq$ key length ≤ 256, typically between 5 and 16, corresponding to a key length of 40 – 128 bits. First, the array "S" is initialized to the identity permutation. S is then processed for 256 iterations in a similar way to the main PRGA algorithm, but also mixes in bytes of the key at the same time. First stage of KSA algorithm steps as explained as following.

1). Initialize the variable length key "i" of size from 0 to 255.
2). Initialize the key matrix "S[i]" as per the size of the input key.
3). Initialize the state table of fixed size 256 bytes from the value 0 to 255 in ascending order.
4. Using the key matrix of variable size done by the permutation on the "S" table
5. Output of the KSA, the final "S" table after swap operation.

KSA algorithm

```
for i from 0 to 255
 S[i] := i
endfor
j := 0
for i from 0 to 255
 j := (j + S[i] + key[i mod key length]) mod 256
swap (&S[i],&S[j])
endfor
```

Many stream ciphers are based on linear feedback shift registers (LFSRs), which while efficient in hardware are less so in software. The design of RC4 avoids the use of LFSRs, and is ideal for software implementation, as it requires only byte manipulations. It uses 256 bytes of memory for the state array, S[0] through S[255], k bytes of memory for the key, key[0] through key[k-1], and integer variables, i, j, and k. Performing a modulus 256 can be done with a bitwise AND with 255 (or on most platforms, simple addition of bytes ignoring overflow). The next stage of the algorithm known as Pseudo-Random Generation Algorithm (PRGA), in this stages basically used to generate the output key stream that used to encrypt and decrypt the data by XORing operation. The algorithm description as follows.

B. Pseudo-Random Generation Algorithm (PRGA).

```
int i=0, j=0
for j from 0  to  255)
for i from 0  to  255)
i=(i+1) mod 256
end for

j=(j + s[i]) mod 256
swap (s[i], s[j])
end for
output= s[ s[i] + s[j] ] mod 256]
```

Simulation Result and Discussion

In this section, we discuss the result and simulation of the standard RC4 algorithm. The implementation of the algorithm has performed in the java programming. Java code writes in the Eclipse java editor and java application implementation tool.

Implementation Output Result

Here it describes the Encryption and decryption output of RC4 algorithm. The output image of the algorithm is showing the inputting plaintext and key length in between 1 to 256 and then plaintext convert into the cipher text during encryption process and cipher text convert back in to plaintext during decryption process. Let's see the implementation output of the algorithm.

RC4 Algorithm Output

```
enter key b/w 0 to 255   100
plaintext is =vijaygraramamohanreddyjntuaapi
ciper text is =
 ?  '  J  ? ÷  d B  §vãfOj%Ox□ ?  z  f {ã  WÚ±;
nano time  96799
used memory is bytes: 209856
plain text is vijaygraramamohanreddyjntuaapi
```

Result Analysis

The analysis of RC4 algorithm is based on defined parameters. ie first we made performs analysis on the collected data and finalized the resulted data. Then prepare the graphical simulation result on the parameter analysis of encryption time, memory utilization of algorithm. In this analysis, we describe the encryption time in nano seconds taken by the algorithm during encrypt the different sized data. To done this analysis, first write the code of the entire algorithm in java, where eclipse java editor tool used and to calculate the time, write the code in java and calculate the encryption time in nano seconds.

Table 1: RC4 Encryption Time

Data Size	Encryption Time
100	132139
200	202508
300	227928
400	333952
500	390177

Analysis Conclusion

As shown in figure 3, we get the graphical representation of RC4 encryption time by using data size verses encryption time for our proposed security system using RC4 algorithm. The encryption time in cloud computing is considered as one of the major factor and so once when the time is reduced better performance can be obtained which results in providing improved security measures in much reduced time interval.

RC4 used over the different types of networks, this proposed algorithm can use the Internet application like E-Commerce, in the healthcare case, for example, a medical center would be the data owner who stores millions of healthcare records in the cloud. It would allow data consumers such as doctors, patients, researchers and etc, to access various types of healthcare records under policies admitted by HIPAA.

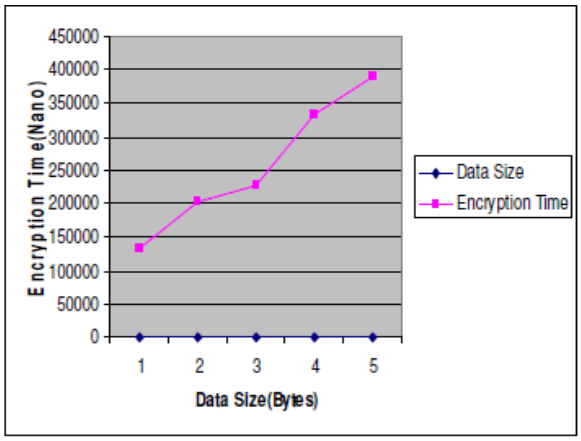

Figure3: Graphical Representation of RC4 Encryption Time.

To enforce these access policies, the data owners on one hand would like to take advantage of the abundant resources that the cloud provides for efficiency and economy; on the other hand, they may want to keep the data contents confidential against cloud servers.

VI. CONCLUSION

Analyzing the trusted computing in the cloud computing environment and the function of trusted Computing platform in cloud computing. The advantages of our proposed approach are to extend the trusted computing technology into the cloud computing environment to achieve the trusted computing requirements for the cloud computing and then fulfill the trusted cloud computing.

TCP is used as the hardware base for the cloud computing system. TCP provides cloud computing system some important security functions, such authentication, communication security and data protection. Related methods for these implementations are proposed.

REFERENCES

1. B.BazeerAhamed, S. Syed Sabir Mohamed, "Implementation of Trusted Computing Technologies in Cloud Computing" International Journal of Research and Reviews in Information Sciences(IJRRIS),Vol. 1, No. 1, March 2011.pp 7-9
2. P radeep Kumar,Vivek Kumar Segal, Durg Singh Chauhan, "Effective Ways of Secure, Private and Trusted Computing", International Journal of Computer Science Issues (IJCSI), vol8, Issues3,No2,May2011 ,pp412-421.
3. Jason Reid Juan M. González Nieto Ed Dawson, "Privacy and Trusted Computing", Proceedings of the 14th International Workshop on Database and Expert Systems Applications, IEEE, 2003
4. Balakrishnan.S,Saranya.G,Shobana.S,Karthikeyan.S,"Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud". International Journal of Computer Science and Technology Vol. 2, Issue 2, June 2011,pp398-400.
5. T.W Edgar, S.L Clements"Cryptographic Trust Management Design Document", U.S. Department of Energy, Pacific Northwest National Laboratory, Vol. 2, Version 1.1, January 2010, pp1.1-17.2.
6. Abhishek Mohta ,Ravi Kant Sahu,Lalit Kumar Awasthi, " Robust Data Security for Cloud while using Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), Volume 2, Issue 2, February 2012,pp1-5
7. David A.Fisher "Trust and Trusted Computing Platform" Technical Note, Software Engineering Institute, January 2011.
8. Xiao-Yong Li , Li-Tao Zhou ,Yong Shi and Yu Guo, "A trusted computing environment model in cloud architecture", International Conference on Machine Learning and Cybernetics (ICMLC), July 2010, Volume 6, pp. 2843-2848
9. Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control: http://www.parc.com/content/attachments/ControllingDataInTheCloud-CCSW-09.pdf
10. Xuan Zhang Wuwong, N. Hao Li Xuejie Zhang, "Information Security Risk Management Framework for the Cloud Computing Environments" IEEE 10th International Conference Computer and Information Technology (CIT), 2010, pp. 1328 – 1334.