International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 5, Issue 2, 2018, PP 17-21
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
DOI: http://dx.doi.org/10.20431/2349-4859.0502003
www.arcjournals.org

Security of Data in Cloud Using Trusted Computing

Vishal Choudhary[1], Dr. Vijay Tiwari[2*]

[1,2]Computer Science and Engineering Centre For Advanced Studies, AKTU Luck now, India

***Corresponding Author:** **Dr. Vijay Tiwari,** Department of computer science & Engineering, Centre for Advance Studies, AKTU Luck now, India*

Abstract: *Cloud computing is a collection of computing systems and servers in which software and other assets are shared publically from the internet. This is another approach to utilize the process, store and offer Data from a system found in any place on planet. Be that as it may, this makes Data unsafe and vulnerable. In this paper, we talk about some security issues in scattered computing and examine a few strategies to enhance security. To do so, we incorporate trusted figuring and distributed computing to enhance security. What's more, to secure content records by executing two fold cryptography calculations.*

Keywords: *cloud; computing security; TCP; TSS.*

1. INTRODUCTION

Cloud Computing came from Grid Computing. Cloud Computing is the service, very much on-demand technology, from application to storage and processing on the internet. Generally companies rent access from cloud service providers to store their data instead of owning their own computing cloud. By renting from cloud service providers, IT infrastructure avoids the cost and complexity of owning and maintaining their data, they simply pay to Cloud Service Providers when they use it.

Since in Cloud Computing all the data travelling between your network and whatever service you are accessing in the cloud is going through internet. That's why security of the data is our major concern. Because that data should be sensitive information about the company or organization. And after storing the data on cloud, accessing of data should be after proper authentication of user. To do so, in this paper we propose Double encryption of text files while storing and accessing of data. A set of software and hardware in the trusted computing is called Trusted Computing Group. And also to ensure Security, Confidentiality, Reliability, Availability, Safety and Integrity. We introduce Trusted Computing Platform (TCP) based on Trusted Platform Module (TPM) into cloud computing system.

Authentication, Confidentiality and Integrity will be taken care by Trusted Computing Platform in cloud computing environment. We also introduce Trusted Platform software Stack (TSS), on which cloud computing application use the security function of Trusted Platform Module. There are two services provided by TCP i.e.

- Authenticated boot, this service finds out which OS is running on computer and acknowledge application about it and also keeps a log of boot process.
- Encryption, this service lets data to be encrypted and decrypted in the same configuration of machine; if machine's configuration is different it won't let data to be decrypted.

In Section II, we will discuss some challenges to Cloud Computing. And in section III, we will discuss what the proposed system is and its architecture. Section IV will see how the proposed system works and helps in authenticating users. Section V also helping in minimizing one of the issue in cloud computing by developing trustful relationship for mutual action. In Section VI, will see the interfaces used between the proposed hardware and application. In this Section VII, we will see how cryptographic algorithms secure the text files stored in cloud when used sequentially.

2. SOME MAJOR ISSUES FACED BY CLOUD COMPUTING SECURITY ARE AS FOLLOWS

Well, Security is the top prior issue in everyday computing, because Data stored on cloud computing could be sensitive data of the company or organization.

- Users, resources join the cloud dynamically so there should be a trustful relationship among them to handle dynamic changes. Therefore developing healthy relationship among them is again a challenge for cloud computing
- In the cloud computing, anyone having credit card or debit card can register for cloud and use the service due to which hackers, spammers can attack the system.
- Owner of data uses software interface of APIs to connect with cloud service and the management and monitoring of services generally done using these interfaces. They may expose organizations to threats such as password, clear text authentication if they are using weak APIs.
- Even trusted employee can leak the sensitive information stored on the cloud.
- Data loss could be possible due to insufficient authentication, authorization and audit controls. Data loss has direct impact on business or can ruin repudiation of brand and customers 'morale.

3. Trusted Computing Platform And Its Architecture

Trusted computing technology proposed by Trusted Computing Group. Trusted Computing System implements procedure into the core operations instead of add-on security applications.

Trusted Computing system cryptographically sealed off the sensitive data part of the computers as it works through combination of software and hardware. TPM maintains the decryption keys. A word Trusted means, "A trusted component, operation, or process is one whose behavior is predictable under almost any operating condition and which is highly resistant to subversion by application software, viruses, and a given level of physical interference". Trusted computing functions can be supported by adding hardware to each computer and then special Trusted computing operating system becomes interface between hardware and any trusted computing enabled applications. Trusted computing designed to improve security, provide privacy and truth in the personal platform. To improve security and privacy, we integrate trusted computing services into the existing cloud computing services.

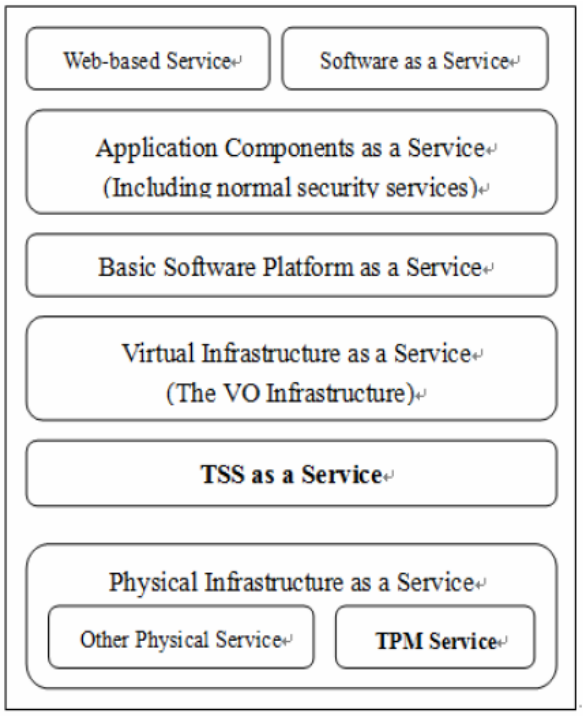

Figure1. *The Architecture of Cloud Computing Based on TCP*

In fig.1, Upper layer services can acquire security services provided by TPM through TSS. TSS communicates directly to TPM. It is a computer chip (microcontroller) that can securely store artifacts used to authenticate platform.

4. Authentication Of User In TCP System

This authentication step is very much important for security point of view. User give their personal identity to cloud administration to join the cloud. Now we introduce TCP in the process of

authentication in cloud, since TPM is an independent hardware based on TCP. In cloud computing, system classify them into several classes or groups according to their goal and behavior and their type of data, they want to store on cloud. So in order to access to the cloud, they have to register themselves into one or more classes groups. After registering, they will get some unique ID and further to access data they should come with full ID including personal identity. TPM is having a private master key which will be used for the protection of data stored in cloud. Since hardware certificate is stored in TPM so it is impossible to crack it. So when user wants to join cloud, it binds their personal ID used for TCP, standard certificate such as X.509 got from CA. Cloud has some mechanism to verify this information for each user. Hardware maintains a "MASTER SECRET KEY" for each machine and uses the master secret key to generate unique sub-key for every possible configuration of that machine. Resulting decryption would be done in the same state of machine as it was during the encryption.

5. Developing Trustful Relationship For Mutual Action

Trusted Computing calculates cryptographic hash code in the Boot process in ROM and maintains a Tamper-resistant log and this process of calculating log goes on. Resulting each chunk of code adds to Tamper-resistant log and the next hash of next chunk will be loaded. This continues until complete OS is booted and gives which OS is running on the system. This configuration of OS's certificate will be given to any recipient, user or program running in cloud. Further recipient verifies the certificate. This way we developed a trustful relationship among ones which have mutual action.

TPM generates some random number and further create session keys using these random numbers. Generated random numbers using physical hardware have much better characteristics than those which are generated by software programs.

6. Software Interface And Services

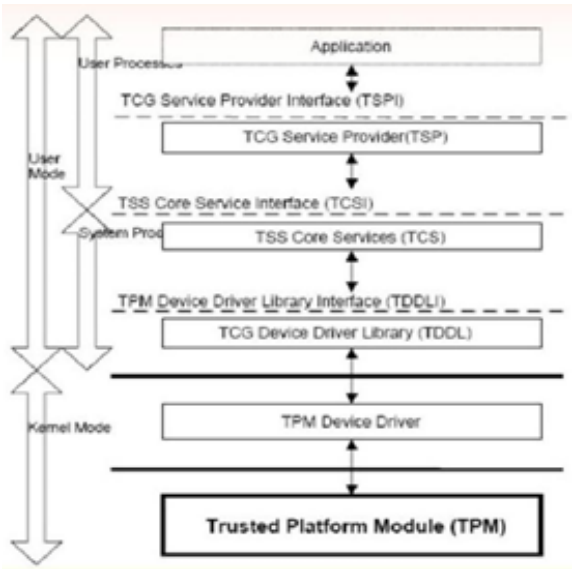

Figure2. *TCG software layering*

Since TSS is an interface between up applications and low hardware. TSS is composed of two layers, one is TSS service provider (TSP) and other one is TSS core services (TCS). The application interacts with TSP and it provide some basic security funtions and then send calls to TCS. TCS also stores credentials like keys associated with platform. This also ensures that all multiple TSS service providers on a single platform perform common behavior. After successful authentication of cloud users, authorization is taken care by TSP. Since TPM is an independent hardware, TCG DEVICE DRIVER LIBRARY (TDDL) is necessary between TSS and TPM. TDDL converts those called functions to TPM orders. Now TPM process them and then send results back to upper layer. In fig.2, TDDL is user mode interface and has more advantages than kernel mode interface. This also ensures efficient uses of applications and resources. Since all things are around TPM hardware, so every command that affect security and privacy of data and resources must be authorized. There are 2 types of commands, i.e.

- Informational commands, these commands contain no
- Security or private information example. TPM_GetCapability functions used for the retrieval of manufacturing information like model name, part number.
- Privacy relevant commands needed to configure command validation.

7. SECURITY OF TEXT FILES IN CLOUD

In this system, we uses DES and RSA algorithm to encrypt the data when owner uploaded on cloud and vice-versa when download file form cloud.

In fig.3, During the encryption phase of text files, upload the text file then implement DES algorithm to generate first level encryption and implement RSA to generate second level encryption and finally store cipher text on cloud.

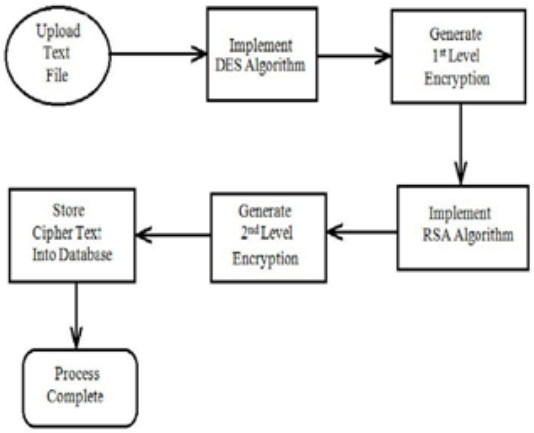

Figure3. *Block Diagram of Multilevel Encryption*

In fig.4, now during decryption, first we read cipher text files from database and then implement RSA algorithm to achieve first level decryption and then apply DES to achieve second level decryption.

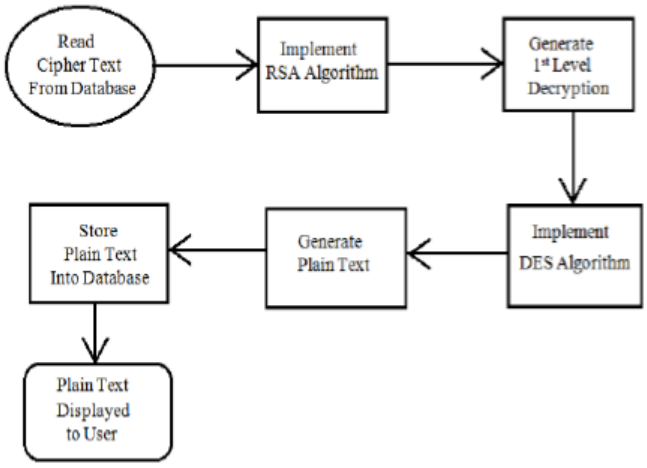

Figure4. *Block Diagram of Multilevel Decryption*

In this system, we have used two differences sequentially to minimize the security issues in personal cloud storage.

8. CONCLUSION

In this paper, initially we discussed the challenges to cloud computing and then proposed the trusted computing in cloud to overcome those challenges. We proposed TPM which is an independent hardware, based on TCP. Later we discussed various functions of TCP. TSS an software interface needed between TPM and up applications. TDDL library interface needed in the TSS software.

Then see how text files can be secure in cloud using cryptographic algorithm RSA AND DES implementing one after the other.

REFERENCES

[1] Zhidong Shen Li Li, Fei Yan Xiaoping Wu, "Cloud Computing System Based on Trusted Computing Platform", 2010 International Conference on Intelligent Computation Technology and Automation.

[2] Zhidong Shen, Qiang Tong, "The Security of Cloud Computing System enabled by Trusted Computing Technology", 2010 2nd International Conference on Signal Processing Systems (ICSPS).

[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] Trusted Computing Group (TCG), "TCG Specification Architecture Overview Specification Revision 1.2", April 28, 2004

[5] TCG, TCG Specification Architecture Overview, Specification Revision 1.4, 2nd August 2007, http://www.trustedcomputinggroup.org

[6] "Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1b", Published by the Trusted Computing Group, 2003.

[7] Balachandra Reddy Kandukuri, Ramacrishna PaturiV, Atanu Rakshi, "Cloud Security Issues", 2009 IEEE International Conference on Services Computing, pages(s):517-520.

[8] N. Santos, K. P. Gummadi, and R. Rodrigues. Towards trusted cloud computing. In USENIX HotCloud, 2009.

[9] Shakeeba S. Khan, Prof.R.R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms" International Journal of Innovative Research in Computer and Communication Engineering , Vol. 3, Issue 1, January 2015

[10] AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, pp.3033-3037, May-Jun 2012.

[11] Tharam Dillon, Chen Wu and Elizabeth Chang, "Cloud Computing: Issues and Challenges", 2010 24th IEEE International Conference on Advanced Information Networking and Applications

[12] Randeep Kaur, Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (ISSN 2319 - 4847),Volume 3 Issue 3, pp.171-176, March 2014.

[13] Neha Jain and Gurpreet Kaur 'Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, pp. 316-321, 2012.

[14] Kevin Curran, Sean Carlin and Mervyn Adams, "Security issues in cloud computing", Elixir Network Engg.38 (2011), pp.4069-4072, August 2011.

[15] Puneet Jai Kaur, Sakshi Kaushal, "Security Concerns in Cloud Computing", Communication in Computer and Information Science Volume 169, pp.103-112, 2011.

[16] Priyanka Arora, Arun Singh, Himanshu Tyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal, pp.179-183, 2012.

Citation: *Vishal Choudhary & Dr.VijayKumarTiwari, (2018)" Security of Data in Cloud Using Trusted Computing", International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), 5(2), pp.17-21. DOI: http://dx.doi. org/10.20431/2349-4859.0502003*