ISSN 2348 – 9928
IJAICT Volume 4, Issue 6, June 2017 Doi:01.0401/ijaict.2014.08.02 Published on 05 (6) 2017

ENHANCE THE CLOUD COMPUTING SYSTEM THROUGH TRUSTED COMPUTING TECHNOLOGY

Mr. K. Somasundaram, Mr. J. Pravin Sam , Mr. R. Jayanthan, Mr. R. Ramachandran

Assistant Professor,
Panimalar Engineering College,
Chennai, Tamilnadu, India

Abstract- ***Personal Computers utilize a local server or else the hard disk to handle, store and process data. Cloud is a group of computers and servers that are openly reachable via Internet. Cloud Computing is a fundamentally novel conception that influence the power of internet to process, accumulate and split data from a network of remote servers positioned wherever in the world. That is an excellent approach to divide several kinds of distributed resources, except it also makes security harms more ambiguous and additional significant for users than ahead of. This paper analysis various security services in cloud computing surroundings and a technique to erect a trusted computing environment for cloud computing arrangement by integrating the trusted computing proposal into the cloud computing structure. Trusted Computing Platform (TCP) representation can pick up the cloud computing safety measures and will not carry much difficulty to users. In this representation, some main security services including validation, integrity and secrecy are provided in the cloud computing structure.***

Keywords: ***Cloud Computing, Trusted Computing Platform, Trusted Service, Trusted Computing.***

I. INTRODUCTION

Cloud computing is an internet based progress and make use of computer technology. Cloud computing provides the approach to distribute the distributed resources and services that fit into dissimilar organizations or sites. Given that cloud computing distributes distributed resources through the network in the open environment, so it makes security trouble significant for us to enlarge the cloud computing relevance. In this paper, notice to the security requests in cloud computing environment. It is a technique to make a trusted computing environment for cloud computing system by integrating the trusted computing proposal into cloud computing scheme. A model system in which cloud computing system is shared with a trusted computing platform through the trusted platform module. In this replica, a few main security services, including validation, confidentiality and reliability, are in cloud computing system.Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers over a network (typically the Internet). Cloud computing is an rising computing paradigm in which property of the computing infrastructure are provided as services in excess of the Internet,where a huge pool of systems are associated in private or public networks, to offer enthusiastically scalable infrastructure for appliance, data and file storage. With the arrival of this technology, the expenditure of computation, appliance hosting, content storage and release the summary significantly. Cloud computing is a realistic approach to practice direct cost remuneration and it has the possible to convert a data center from a capital-intensive set up to a changeable priced environment[3]. The idea of cloud computing is based on a extremely fundamental principal of reusability of IT capabilities. The variation that cloud computing brings compared to conventional concepts of grid computing, distributed computing, or autonomic computing is to expand horizons across managerial limitations.

The Cloud pertains to all the papers or records kept by servers from isolated locations that can be accessed all the way through the Internet. Storing data from end to end the Cloud makes it easy for all the parties fretful to be able to regain the information they need. Within the Cloud, users may be proficient to accumulate and organize their files for individual use, or for other users to be able to make use of it. Cloud computing is a catchall expression that covers virtualized operating systems running on virtual hardware on innumerable numbers of physical servers. It is a hypothesis where tasks are assigned to a permutation of associates, software and services accessed over a network.

Trusted Computing (TC) is a technology developed and promoted by the Trusted Computing Group. The TCG project is recognized by a amount of names. Trusted computing was the unique one, and is immobile used by IBM, whereas Microsoft calls it trustworthy computing and the Free Software Foundation calls it treacherous computing. I'll just call it TC, which you can pronounce according to taste [13].Trusted computing is a lane term that refers to technologies and

proposals for resolving computer protection problems through hardware enhancements and related software modifications. Numerous chief hardware manufacturers and software vendors, communally identified as the Trusted Computing Group, are cooperating in this enterprise and have come up with detailed plans. The TCG develops and promotes provision for the protection of computer resources from intimidation posed by spiteful entities without infringing on the rights of end users [4].

The applications of cloud Computing are sensibly unbounded. With the precise middleware, a cloud computing system could implement all the programs a normal computer could run. Everything from generic word processing software to personalized computer programs planned for a specific company could work on a cloud computing system [2].

In a world that sees new scientific trends bloom and fade on nearly a daily basis, one new trend promises more prolonged existence. This trend is called cloud computing, and it will amend the way you use your computer and the internet. Cloud computing portends a foremost transform in how we store in sequence and run applications. Instead programs and records on an individual's desktop computer, the whole lot is hosted in the cloud a tenuous collection of computers and servers accessed through internet [12]. Cloud computing lets you access all your applications and document from anywhere in the world, glacial the margins of the desktop and making it easier for group members in different locations to team up. Cloud computing despite the fact that it appears as network computing, it is not. With network computing applications or documents are hosted on a distinct company's server and accessed over the company's network. Cloud Computing starts getting different here. It encompasses multiple companies and multiple networks. Cloud services and storage are handy from anywhere in the world over the Internet connection. Cloud computing is also not an outsourcing process, where a company farms out its computing services to an external firm.

Cloud Computing is a sprouting technique of Global Computing. Here the user can hook up to the internet and start using all the mandatory resources without a client side application installed on user's system. This eliminates the Physical storage mechanism on the client machine. Cloud computing differs from the standard client-server model by providing applications from a server that are executed and managed by a client's web browser. Centralization gives cloud service providers inclusive control over the versions of the browser-based applications provided to clients, so no need for version upgrades or license management on individual client computing devices. Traditional business applications have always been very intricate and classy.

II. LITERATURE REVIEW

2.1 Cloud Computing

Cloud computing provides calculations, software, data contact, and storage services that do not involve end-user acquaintance of the physical location and configuration of the system that delivers the service.

2.2 Trusted Computing

The Trusted Computing Group (TCG) planned a set of hardware and software technologies to facilitate the construction of trustworthy platforms. The Trusted Computing Platform (TCP) will be used in verification, privacy and integrity in cloud computing environment [15]. A Trusted Platform is a computing platform that has a trusted element, possibly in the structure of built-in hardware, which it uses to generate a foundation of trust for software processes [3].

The Trusted Computing Group projected a set of hardware and software technologies to enable the construction of trusted platforms. The Trusted Computing Platform will be used in verification, secrecy and integrity in cloud computing environment TC is notorious because it is technically possible not just to secure the hardware for its owner, but also to secure against its owner [17]. In recent years, amplified trust on computer security and the regrettable fact of lack of it, mostly in the open-architecture computing platforms, have inspired many efforts prepared by the computing industry.

Since one of the major issues facing computer technology today is data security, and the problem has gotten inferior because users are working with receptive information more often, while the number of threats is increasing and hackers are budding new types of attacks, many technology researchers advocate development of trusted computing systems that integrate data security mechanism into their core operations, rather than implementing it by using add-on applications It is safer remote access through a permutation of machine and user authentication and protects against data leakage by confirmation of platform integrity prior to decryption[18].

2.3 Trusted Computing Services

Trusted Computing Platform operates in the course of a permutation of software and hardware.TCP provides following services,

Authenticated boot: An authenticated boot service monitors what operating system software is booted on the computer and also enlighten which operating system is in a row. Each site in the cloud computing system will trace the visitor's information. So by using the TCP mechanism in cloud computing, the

sketch of participants can be known by the cloud computing trace mechanism.

Encryption: Encryption is a process of translating the cipher text into plaint text. This function lets figures be encrypted in such a system that it can be decrypted only by a certain machine, and only if that machine is in a certain configuration. The encryption is an additional chief mechanism in our design. This service is built by a blend of hardware and software application.

Authentication: Authentication is the act of confirming the reality of an attribute of a datum or entity. Authentication provides the access permission to only the endorsed users and restricts the illicit users.

Confidentiality: The information belongs to dissimilar owners in the cloud computing resources should be open to the trusted objects. Illicit people or other entities should be forbidden from that information.

Integrity: We cannot alter the novelty of the information so integrity is regarded as the candour and reliability or precision of one's actions. Integrity can be regarded as the reverse of duplicity, in that it regards domestic consistency as a virtue, and suggests that parties holding actually inconsistent values should account for the discrepancy or amend their attitude.

III. ARCHITECTURE

We can develop the safety of cloud computing system using trusted computing technology. Trusted Computing (TC) is a technology urbanized and promoted by the Trusted Computing Group. The stretch is engaged from the field of trusted systems and has a focused implication. With Trusted Computing, the computer will constantly act in usual ways, and those behaviours will be enforced by hardware and software. This mechanism is an excellent alternative because the web service technology has been well established in the network-computing environment.

IV. TRUSTED COMPUTING TECHNOLOGY

4.1 Basic Concepts in the Trusted Platform Model

TPM can impose security policies on hierarchies of secret keys to preserve them from software attacks by several remote attackers. The Trusted Computing Platform Alliance has available papers that stipulate how a Trusted Platform must be constructed. On each Trusted Platform is a Trusted Subsystem, which contains a Trusted Platform Module , a Core Root of Trust for Measurement, and support software.

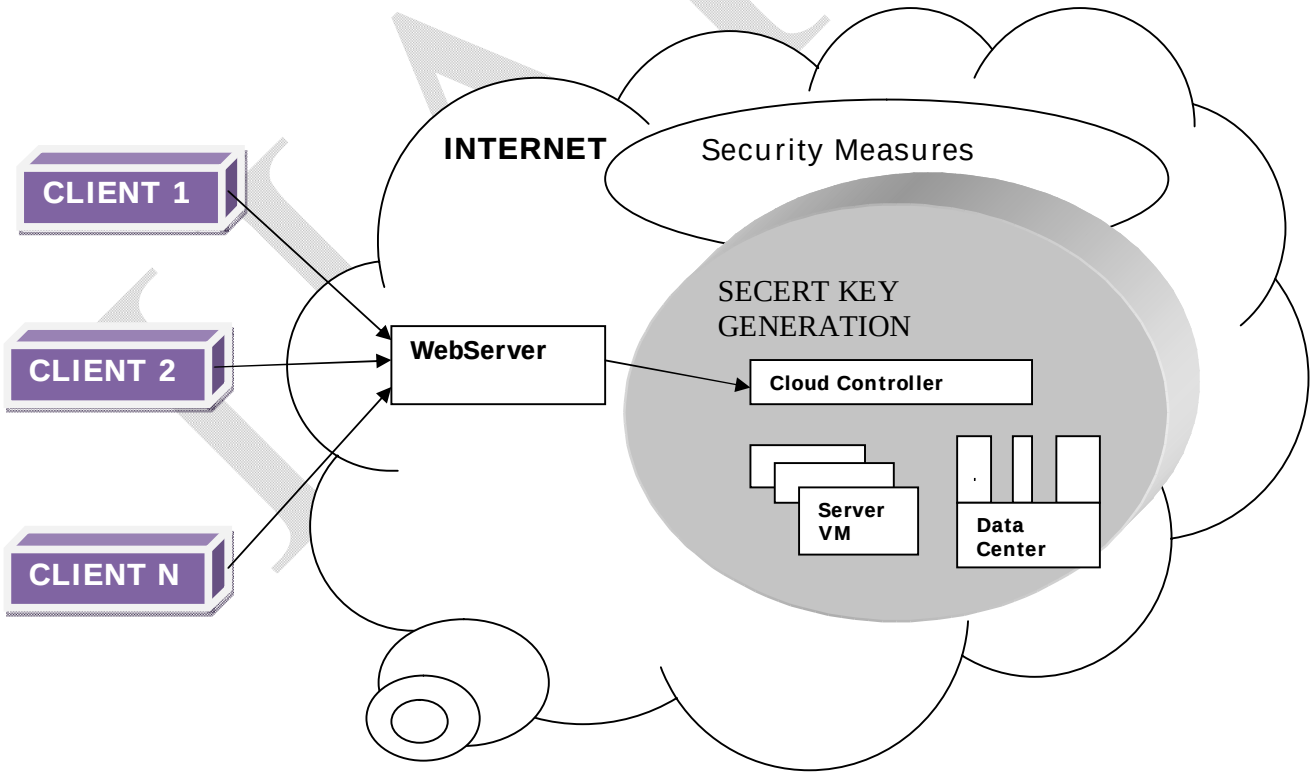

Fig 1: Trusted Cloud Computing

The TPM is a hardware chip that's taken, apart from the most important platform CPU. The CRTM is the first software to run during the boot process and is rather physically located within the TPM, even if this isn't essential. The TSS performs a range of functions, such as those crucial for communication with the rest of the platform and with other platforms [15].

The TSS functions don't necessitate to be responsible, but are yet mandatory, if the display place is to be trusted. In addition to the Trusted Subsystem in the physical Trusted Platform, Certification establishment is centrally implicated in the manufacture and procedure of Trusted Platforms (TPs) in order to assure that the TP is legitimate [13]. Readers with a background in information security know that a Trusted Computing Base is generally the set of functions that endow with the security properties of a platform.

The Trusted Computing Platform in a Trusted Platform is the permutation of the Trusted Subsystem and supplementary functions. Since, the Trusted Subsystem is a part of the utility of the Trusted Computing Base of conventional, secure computers, which would normally incorporate both productions with secrets and using secrets. Crucially, however, the Trusted Subsystem contains some functions not initiate in a conventional Trusted Computing Platform. Conventional secure computers endow with formal support that a TCB in certain states actually can be trusted [15].

4.2 The Trace of the User's Behavior

The users have complete information about their identity, the cloud computing arrangement can utilize some method to sketch the users and get their resource. Because in the Transmission Control Protocol the user's individuality is proven by user's individual input and this device is incorporated in the hardware, such as the BIOS and Trusted Platform Model. It is very rigid to the user to make illusory for their identity information. Before the circulated machine cooperates to do implausible, they should designate their local information to the far-flung position. When the user login the cloud computing system, his distinctiveness information should be recorded and verified at first. Secured communication and secured messages can be transported, implicit, and manipulated by standard Web services tools and software. This mechanism is a fine option because the web service technology has been well recognized in the network-computing environment. Even the mechanism for the cloud computing security has lots of merits now, but readily available are still several disadvantages. Each site in the cloud computing system will trace the visitor's information. So if the TCP mechanism is incorporated into the cloud computing, the sketch of the participants, counting the users and other resources, can be known by the cloud computing trace mechanism. Then, if the participants do some spiteful behavior, they will be tracked and punished. In order to attain the trusted computing in the cloud computing system, we should have the mechanism to identify not only what the participants can do, but also what the participant have completed. So, the monitoring task should be incorporated into the cloud computing system to manage the participants' behavior. In reference monitors have been used in the operating system for more than several decades [15].

4.3 Trusted Cloud Computing based on TCP

The trusted computing mechanism can afford an approach that can facilitate to establish a security cloud computing environment. The form of trusted computing is initially intended to offer the privacy and trust in the individual platform and the trusted computing platform is the support of the trusted computing. While the internet computing or network computing has been the chief computing from the end of the last century, the demonstration of trusted computing is being developed to the network computing, predominantly the distributed systems environment.

The cloud computing is a hopeful distributed system form and will act as a vital role in the e-business or research environments. As web service technology has developed quickly and have been used largely, cloud computing system could develop to cloud computing services, which integrates the cloud computing with web service technology. So we could widen the trusted computing mechanism to cloud computing service systems by integrating the TCP into a cloud computing system. The trusted computing platform offers the basis for trusted connections to occur, and trusted computing technologies must consent to stakeholders to articulate policies and have those policies negotiated and enforced in any execution environment.

4.4 Trusted Hardware

Trusted Computing as it exists these days is defined by the stipulation of the Trusted Computing Group. The Trusted Platform Module, is incorporated into frequently available general principle hardware, through hundreds of millions of platforms shipped so far away. Similar to a smart card, a TPM features cryptographic primitives, but is actually bound to its host device. It contains a tamper resistant incorporated circuit implementation public key cryptography, key generation and random number prediction. By means of these gears, the TPM

can impose defense policies on hierarchies of furtive keys to defend them from software attacks by any remote attacker [11].

TPM can be used to carry out cryptographic signatures on user-provided data, using hardware-protected confidential keys. However, due to inadequate TPM memory, keys have to be swapped out of the TPM when not in use. To defend these keys, a parent storage key specified on key design is used to enclose the concealed part of the child key when it is exported from the TPM. At the top of the key hierarchy is the storage root key shaped when taking ownership of the TPM. Keys are assigned a user supplied secret, which is used in numerous authentication protocols, and optionally a system state that has to be provided when using the key for cryptographic operations [12].

4.5 Authentication cloud computing environment with Trusted Computing Platform

The dissimilar entities in a cloud computing environment can plead to join the CLOUD. Then the first step is to demonstrate their identity to the cloud computing configuration supervision. Because cloud computing should entail a huge amount of entities, such as users and resources from dissimilar sources, the confirmation is imperative and elaborate. Allowing for this, we exercise the Trusted Computing Platform to assist to process the authentication in cloud computing. It can disregard the attack from software, and even the hardware attack. The TPM includes a private master key which can endow with defend for other information accumulate in cloud computing system. Since the hardware certificate can stock up in TPM, it is hard to attack it. So TPM can afford the trust root for users.

The cloud computing service should present, which task it will give the authorization, when the cloud computing service notifies itself to the cloud -computing environment. So the user will able to recognize whether he could make admittance to that cloud computing service before his action. The encryption is an added major mechanism in our design. This function lets data be encrypted in such a manner that it can be decrypted only by a definite machine, and single if that machine is in a convinced configuration. This service is built by a permutation of hardware and software application. The hardware maintains a master secret key for each machine, and it uses the master secret to breed a unique sub key for every feasible configuration of that machine. As a result, data encrypted for a fussy configuration cannot be decrypted when the machine is in a different configuration [17].

When one machine wants to bond the cloud computing, it will show its certificate and produce the session key with other co-operators acquire using the exclusive sub-key. If the configuration on the local machine is distorted, the session-key will also be not useful. So in the distributed environment, we can exploit this function to spread data to a remote machine and this data can be decrypted when the remote machine has certain configuration [18].

4.6 TSS and Cloud Computing System

TSS components are the major parts of the TCP enabled cloud computing. It provides basic resources to sustain the TPM. In our design, TSS should be a bridge between the application and the low-hardware.

V. CONCLUSION

This paper analyses the trusted computing in the cloud computing environment and the task of trusted computing platform in cloud computing. The reward of our planned approach is to widen the trusted computing technology into the cloud computing environment to complete the trusted computing requirements for the cloud computing and then fulfill the trusted cloud computing. Trusted Computing Platform is used as the hardware establishment for the cloud computing arrangement. In our design, TCP provides cloud computing system some essential security functions, such as authentication, communication security and data protection. The TCP provides cloud computing a privileged base for attaining trusted computing. But how to incorporate glowing these hardware modules in the cloud computing system is a complicated effort and require further deep research. Now we are booting a model system of trusted cloud computing, which is based on the trusted computing platform and can grant stretchy security services for users. We will make the tangible design more handy and effective in the future**.**

References

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

[2] Cloud Computing, http://en.wikipedia.org/wiki/Cloud_computing, Accessed: 30/08/2011.

[3] Cloud Computing, http://www.techno-pulse.com/ Cloud Computing for Beginners, Accessed: 30/08/2011.

[4] Cloud Security Alliance: Security Guidance Critical Areas of Focus in Cloud Computing, http://www.cloudsecurityalliance.org/guidance/ csaguide.pdf. April 2009.

[5] Dr.Rao Mikkilineni, Vijay Sarathy, "Cloud Computing and the Lessons from the Past", the 18th IEEE international Workshops on Enabling Technologies: Infrasturctures for Colloaborative Enterises, on page(s):57-62, 2009.

[6] Frank E. Gillett, "Future View: The new technology ecosystems of cloud, cloud services and cloud computing" Forrester Report, August 2008.

[7] Glen Bruce, Rob Dempsey, "Security in Distributed Computing", Published by Prentice Hall, Copyright Hewlett-Packard Company, 1997.

[8] ISO/IEC. Information technology - Open Systems Interconnection - Evaluation criteria for information tech-nology, Standard ISO/IEC 15408.1999.

[9] 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.

[10] Martín Abadi, "Logic in Access Control", Proceedings of the 18th Annual IEEE Symposium on Logic in Computer Science (LICS'03), 2003.

[11] Peter Wayner, "Cloud versus cloud – A guided tour of Amazon, Google, AppNexus and GoGrid", InfoWorld, July 21, 2008.

[12] Ronald Toegl, Thomas Winkler, Mohammad Nauman, Theodore Hong, "Towards Platform-Independent Trusted Computing",2009.

[13] Tal Garfinkel, Mendel Rosenblum, and Dan Boneh, "Flexible OS Support and Applications for Trusted Computing", the 9th Workshop on Hot Topics in Operating Systems (HotOS IX), USENIX, 2003.

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

[15] Trusted computing group:http://www.trustedcomputinggroup.org. Accessed: 7/08/2011.

[16] Trusted computing Technology : http://en.wikipedia.org/wiki/ Trusted_ Computing Accessed:7/08/2011.

[17] Trusted computing : http://www.wave.com. Accessed: 10/09/2011.

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