Improving the Security of Cloud Computing using Trusted Computing Technology

P.Senthil[1]
PG Student, Dept of CSE,
CIET, Coimbatore, TN, India.

N.Boopal[2]
Assistant Professor, Dept of CSE,
CIET, Coimbatore, TN, India.

R.Vanathi[3]
PG Student, Dept of CSE,
CIET, Coimbatore, TN, India.

ABSTRACT

Cloud Computing is a collection of computers and servers that are publicly accessible via Internet. It is a significantly new idea that influence the power of internet to process, store and share data from a network of remote servers located anywhere in the world. That is a good way to share a many kinds of distributed resources, but it also makes security problems more complicate and more important for users than before. This paper analyses some security services in cloud computing environment and a method to build a trusted computing environment for cloud computing system by integrating the trusted computing platform into cloud computing system. Trusted Computing Platform (TCP) model can improve the cloud computing security and will not bring much complexity to users. In this model, some important security services including encryption, authentication, integrity and confidentiality are provided in cloud computing system.

***Keywords* - Cloud Computing, Trusted Computing, Trusted Computing Platform, TCPA, Trusted Security Services.**

1. INTRODUCTION

Cloud computing provides a large business model that supports pay-for-use, on-demand and economies-of-scale IT services through the Internet. The Internet cloud working as a service factory that built around virtualized data centers. Cloud Computing platforms are dynamically built through the virtualization with provisioned hardware, software, datasets and networks. Cloud computing is an internet based progress and use of computer technology. It provides the way to share distributed resources and services that be in the right place to different organizations. Since cloud computing share distributed resources via the internet in the open environment, thus it makes security problems important for us to develop the cloud computing application. In this paper, we attention to the security requirements in cloud computing environment. It is a method to build a trusted computing environment for cloud computing system by integrating the trusted computing platform into cloud computing system. A model system in which cloud computing is shared with trusted computing platform with trusted platform module. In this model, some important security services, includes authenticated boot, encryption authentication, confidentiality and integrity, are in cloud computing system[1].

Cloud computing technology 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.Cloud computing is an growing computing paradigm in which resources of the cloud computing infrastructure are provided as services over the Internet, where a large team of systems are connected in private or public networks, to provide dynamically scalable communications for application, data and file storage. With the arrival of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. Cloud computing is a useful approach to experience direct cost benefits and it has the possible to transform a data center from a capital-intensive set up to a variable priced environment[2].

The idea of cloud computing is based on a very fundamental principal of reusability of Information Technology capabilities. The difference that cloud computing brings compare to traditional concepts of “grid computing”, “distributed computing”, “utility computing”, and “autonomic computing” is to extend horizons across organizational boundaries. The Cloud pertains to all the documents or files reserved by servers from remote locations that can be accessed throughout the Internet. Storing data through the Cloud computing makes it easy for all the parties concerned to be able to recover the information they require. Inside the Cloud, users may be able to store and manage their files for personal use, or for other users to be able to utilize it. Cloud computing is a catch-all turn of phrase that covers virtualized operating systems running on virtual hardware on untold numbers of physical servers. It is a computing paradigm where tasks are assigned to a combination of connections, software and services accessed over a network.

Trusted Computing technology was developed and promoted by the Trusted Computing Group(TCG).It is a group of Microsoft, Intel, IBM, HP and AMD which promotes a pattern for a `more secure' Personal Computer. The Trusted Computing Group project is known by a number of names. `Trusted computing' was the innovative one, and is now used by IBM, while Microsoft calls it `trustworthy computing' and the Free Software organization calls it `treacherous computing' which you can pronounce according to taste [16].Trusted Computing Platform Alliance (TCPA),is an initiative started by AMD, HP, IBM, Intel, and Microsoft to implement Trusted Computing.

Trusted computing is a broad word that refers to technology and proposals for resolving computer security problems through hardware enhancements and related software modifications. A number of major hardware manufacturers and software vendors, collectively known as the Trusted Computing Group, are cooperating in this venture and have come up with specific plans. The TCG develops and promotes provision for the protection of computer resources from threats by malicious entities without infringing on the rights of end users. The Trusted Computing Platform provides cloud computing a sheltered base for achieve trusted computing [2]. A Trusted Platform Module (TPM) is a secure portal to potentially infinite amounts of protected storage, even though the time to store and retrieve particular information could ultimately become large.

2. THEORETICAL BACKGROUND

2.1 Cloud Computing

Cloud computing provides computation, software, data access, and storage services that do not necessitate end-user knowledge of the physical location and constitution of the system that delivers the services. The applications of cloud computing are practically unlimited. Through the right middleware, a cloud computing system could execute all the programs a ordinary computer could run. Everything from generic word processing software to personalized computer programs designed for a specific company could work on a cloud computing system [2].In a world that sees new technological trends blossom and fade on almost a daily basis, one new trend promises more prolonged existence. This trend is called cloud computing, and it will modify the way you use your computer and the internet. Cloud computing portends a major change in how we store information and run applications. Instead programs and data on an individual's desktop computer, everything is hosted in the "cloud"-an unformulated assemblage of computers and servers accessed via internet [2].

Cloud computing lets you access all your applications and document from anywhere in the world, baggage the confines of the desktop and making it easier for group members in different locations to collaborate. Cloud computing though it appears as network computing. With network computing applications or documents are hosted on a single company's server and accessed over the company's network. Cloud Computing starts getting different here. It encompasses various companies, various servers, and various networks. Cloud services and storage are accessible from anywhere in the world over the Internet connection. Cloud computing is also not an outsourcing process, where a company farms out (subcontracts) its computing services to an outside firm.

Cloud Computing is a growing method of Global Computing. Here the user can connect to the internet and start using all the required 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 classic client-server model by provide applications from a server that are executed and managed by a client's web browser. Centralization gives cloud service providers complete control over the version 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 complex and expensive.

2.2 Trusted Computing

The Trusted Computing Group (TCG) proposed a set of hardware and software technologies to enable the construction of trusted platforms. The Trusted Computing Platform (TCP) will be used in authentication, confidentiality and integrity in cloud computing environment [14]. Trusted computing Platform is a computing platform that has a trusted component, most likely in the form of built-in hardware, which it uses to create a base of trust for software processes [4]. The Trusted Computing Group proposed a set of hardware and software technologies to enable the construction of trusted platforms. The Trusted Computing Platform will be used in authentication, confidentiality and integrity in cloud computing environment TC is controversial because it is technically possible not just to secure the hardware for its owner, but also to secure against its owner [18].

In recent years, increased confidence on computer security and the unfortunate fact of lack of it, particularly in the open-architecture computing platforms, have motivated many efforts made by the computing industry. In 1999, HP, IBM, Compaq, Intel, and Microsoft announced the formation of the Trusted Computing Platform Alliance (TCPA) that focused on building confidence and trust of computing platform in e-business transactions [15]. In 2003, the Trusted Computing Group was formed and has adopted the specifications developed by TCPA. Because one of the biggest issues facing computer technology today is data security, and the problem has gotten worse because users are working with sensitive information more often, while the number of threats is growing and hackers are developing 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 combination of machine and user authentication and protects against data leakage by confirmation of platform integrity prior to decryption[18].

The Trusted Platform Module is an international standard, hardware security component built into many computers and computer-based goods. The TPM includes capabilities such as machine authentication, hardware encryption, secure key storage, and attestation. Encryption and signing are well known techniques, but the TPM makes them stronger by storing keys in protected hardware storage space. Machine authentication is a core principle that allows clouds to authenticate to a known machine to provide this machine and user a higher level of service as the machine is known and authenticated.

2.3 Trusted Computing Security Services

Trusted Computing Platform operates through a combination of software and hardware.TCP provides following security services,

Authenticated Boot

An authenticated boot service used to monitors what operating system software is booted on the computer and also tell which operating system is running. 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.

Encryption

Encryption is a process of translating the cipher text into plaint text. This function lets data be encrypted in such a way that it can be decrypted only by a certain machine, and only if that machine is in a certain configuration. The encryption is another major mechanism in our design. This service is built by a combination of hardware and software application.

Authentication

Authentication is the act of confirming the truth of an attribute of a datum or entity. Authentication provides the access permission to only the authorized users and restricts the unauthorized users.

Confidentiality

The information belongs to different owners in the cloud computing resources should be open to the trusted objects. Unauthorized people or other entities should be forbidden from that information.

Integrity

In integrity, cannot modify the originality of the information so integrity is regarded as the honesty and truthfulness or precision of one’s actions. Integrity can be regarded as the opposite of duplicity, in that it regards internal consistency as a good feature, and suggests that parties holding apparently contradictory values should account for the inconsistency or alter their beliefs.

2.4 Trusted Components

Trusted computing consist of the following components,

Trusted Platform Support Services:

Trusted Platform Support Services is middleware that act as an intermediate between the TCP and the users.

Trusted Platform Module:

Trusted Platform Module is a security device that Can Store the cryptographic keys.

Core Root of Trust for Measurement:

It is software that can be used to identify the trusted root.

2.5 Need of Trusted Computing

With the ever increasing threat to identities and sensitive information, effective solutions can no longer be based on software only solutions, but on hardware which Trusted Platforms contain[17].Top problems and threats that a Trusted Platform can address:

- Identity theft and impersonation through unprotected passwords and sensitive information.
- Unauthorized network access, such as to a corporate network, a wireless network, or a VPN
- Regulatory compliance issues for strong authentication and data protection.
- Unauthorized access to unprotected files, documents, or email on client PCs or servers.

3. ARCHITECTURE

The architecture was designed to encompass a wide variety of tools and technologies. It provides strong user authentication, blocks the access of unsafe endpoints and coordinates security devices across the enterprise. The Trusted Computing technology is used to improve the security of cloud computing system.

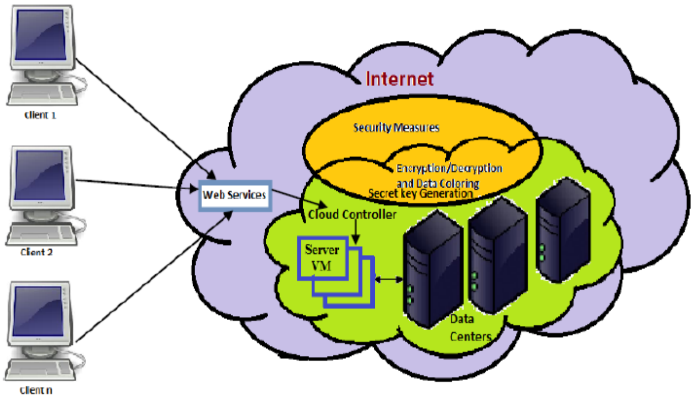

Fig 1. Trusted Cloud Computing

Trusted Computing was developed and promoted by the Trusted Computing Group. The word is taken from the field of trusted systems and has a specific meaning. We can generate the “master secret key” for each machine, and it uses the master secret to generate a unique sub-key for every possible configuration of that machine With Trusted Computing, the computer will constantly behave in expected ways and those behaviours will be enforced by hardware and software. This mechanism is a good choice because the web service technology has been well established in the network-computing environment. We can use the data colouring on varying security levels based on the variable function and apply the method to protect software, documents, images, video and relational databases. The details involved in the colour-matching process, which aims to combine a colured data object with its vendor, whose user identification is also colored with the same expected value depends on the data content, whereas *entropy* and *hyper entropy* add randomness or uncertainty. The colour-matching process assures that colours applied to the user identification match the data colours. This can initiate various trust-management events, including authentication, confidentiality, integrity and Virtual storage supports colour generation, embedding, extraction. Combining secure data storage and data colouring, we can prevent data objects from being damaged, stolen, altered and deleted.

4. TRUSTED COMPUTING TECHNOLOGY

4.1 Trusted Platform Model

TPM can implement security policies on hierarchies of secret keys to protect them from software attacks by some remote attacker. The Trusted Computing Platform Alliance (TCPA) has published documents that specify how a Trusted Platform must be constructed. Within each Trusted Platform is a Trusted (Platform) Subsystem, which contains a Trusted Platform Module (TPM), a Core Root of Trust for Measurement (CRTM), and support software.

The TPM is a hardware chip that’s separate from the main platform CPU(s). The CRTM is the first software to run during the boot process and is preferably physically located within the TPM, although this isn’t essential. The Trusted platform Support Service (TSS) performs a variety of functions, such as those necessary for communication with the relax of the platform and with other platforms [15].The TSS functions don’t require to be trustworthy, but are however required if the platform is to be trusted. In addition to the Trusted Subsystem in the substantial Trusted

Platform, Certification Authorities (CAs) are centrally involved in the manufacture and usage of Trusted Platforms in order to guarantee that the TP is genuine [15]. Readers with a background in information security know that a Trusted Computing Base (TCB) is approximately the set of functions that provide the security properties of a platform.

The TCB in a Trusted Platform is the combination of the Trusted Subsystem (mainly dealing with secrets) and additional functions. As such, the Trusted Subsystem is a subset of the functions of the Trusted Computing Base of conventional sheltered computers, which would normally include both dealing with secrets and using secrets. Crucially, however, the Trusted Subsystem contains some functions not found in a conservative TCB. Conventional secure computers provide formal proof that a TCB in certain states actually can be trusted [15].

4.2 Trace of the User's Behaviours

The users have chock-full information about their identity, the cloud computing system can use some mechanism to trace the users and get their source. Since in the TCP the user's identity is proved by user's special key and this mechanism is included in the hardware, such as the BIOS and TPM. It is very hard to the user to make unreliable for their identity information. Previous to the distributed machine cooperates to do a little, they should attest their neighbouring information to the remote location. When the user login the cloud computing system and his identity information should be recorded and verified at foremost. The cloud computing security can be provided as security services and resources. Security messages and secured messages can be transported, unstated, and manipulated by model Web services tools and software. This mechanism is a good choice because the web service technology has been well established in the network-computing environment. Even the mechanism for the cloud computing security has many merits now, but there are still a number of disadvantages.

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 behaviour, they will be tracked and be punished. In order to achieve the trusted computing in the cloud computing system, we 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' behaviour. In reference monitors have been used in the operation system for more than several decades.

4.3 Cloud Computing based on TCP

The trusted computing technology can provide a way that can help to set up a security cloud computing background. The model of trusted computing is initially designed to provide the privacy and trust in the personal platform and the trusted computing platform is the base of the trusted computing. Because the internet computing or network computing has been the main computing from the ending 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. Trusted computing platform provide the basis for trusted transactions to occur, and trusted computing technologies must allow stakeholders to express policies and have those policies negotiated and enforced in any execution environment.

4.4 Trusted Hardware

Trusted Computing technology as it exists nowadays is distinct by the specifications of the Trusted Computing Group. Hardware component, the Trusted Platform Module, is integrated into commonly available general-purpose hardware, with millions of platforms shipped so far away. Like a smart card, a Trusted Platform Module features cryptographic primitives, but it can be physically bound to its host device. Trusted hardware contains a tamper-resistant integrated circuit implementation public key cryptography, key generation, secure hashing, and random-number generation. To use these components, the Trusted Platform Module (TPM) can enforce security policies on hierarchies of secret keys to protect them from software attacks by any remote attacker.

Trusted Platform Module can be used to perform cryptographic signatures on user-provided data using hardware-protected private keys. However, due to limited TPM memory, keys have to be swapped out of the TPM when not in use. To protect these keys, a parent storage key specified on key creation is used to wrap the private part of the child key when it is exported from the TPM. At the top of the key hierarchy is the storage root key created when taking ownership of the TPM. Keys are assigned a user-supplied secret, which is used in several authentication protocols, and optionally a system state that has to be provided when using the key for cryptographic operations [12].

4.5 Authentication of cloud computing environment with Trusted Computing Platform

Data protection is a more than just a subject of maintenance in the wrong people out of places they shouldn't be and not having valuable records disappear. Data protection is a driven by a host of new legal requirements that protect the customer privacy. It is Critical to data protection will be the safe linking of host CPU and hard drives. Different entities can appeal to join the cloud computing environment. The initial step is to verify 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 TCP is based on the TPM. The TPM is a logic independent hardware [18]. 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.

The cloud computing service should present which role it will give the permission, when the cloud computing service notifies itself to the cloud -computing environment. So the user will able to know whether he could make access to that cloud computing service before his action. The encryption is another major mechanism in our design. This function lets data be encrypted in such a way that it can be decrypted only by a certain machine, and only if that machine is in a certain configuration. This service is built by a combination of hardware and software application. The hardware maintains a “master secret key” for each machine, and it uses the master secret to generate a unique sub-key for every possible configuration of that machine. As a result, data encrypted for a particular configuration cannot be decrypted when the machine is in a different configuration.

When one machine wants to join the cloud computing, it will show its certificate and generate session key with other co-operators buy using the unique sub-key. If the configuration in the local machine is changed, the session-key will also be not useful. So in the distributed environment, we can use this function to transmit data to remote machine and this data can be decrypted when the remote machine has certain configuration.

4.6 Trusted platform Support Service

TSS components are the major parts of the TCP enabled cloud computing. It provides fundamental resources to support the TPM. In our design, TSS should be a bridge between the up-application and the low-hardware. Trusted platform Support Service (TSS) includes two layers, the TSS service provider (TSP) and TSS core services (TCS). The applications call the function of TSP. TSP provides some basic security function modules. These basic modules send calls to TCS. Then TSS converts these calls to according TPM instructions. Since TPM is hardware, the TCG Device Driver Library (TDDL) is necessary. TDDL convert the calls from TCS to the TPM orders.

After the TPM process the order, it will return the results up forward. Each layer gets results from low layer and coverts them to responding results that the up layer needs.

The main issue with the "Cloud" is linked to the responsiveness of information. In a cloud, each of us is completely right to be concerned about the confidentiality and the availability of the information. Tomorrow's world will be based on information. But the future is becoming gradually more doubtful. Information is a critical resource that requires severe controls and protection.

4.7 Trusted Computing Benefits

Trusted Computing technology creates a safer environment in cloud computing. It provides Safer Remote Access through a Combination of mechanism and User Authentication. Trusted computing Protects against data leakage by confirmation of platform integrity prior to encryption and decryption. The Hardware Protection for Encryption and Authentication Key is used by Data (Files) and Communications (Email, Network Access). The Hardware Protection for individually Identifiable Information such as User Ids and Passwords. Lowest Cost Hardware Security Solution: No Token to Distribute or Lose, No Peripheral to Buy or Plug In, No Limit to Number of Keys, Files or IDs Protected.

- Trusted Computing Protect Business Critical Data and Systems.
- Secure Authentication and Strong Protection of User IDs.
- Establish Strong Machine Identity and Integrity.
- Ensure Regulatory Compliance with Hardware-Based Security.
- Trusted Computing Reduce the Total Cost of Ownership through "Built In" Protection.

5. CONCLUSION AND FUTURE WORK

This paper analyzed and finds the role of trusted computing platform in cloud computing. Trusted Computing Platform is used as the hardware foundation for the cloud computing system. Trusted Computing Platform provides cloud computing system with some imperative security functions, which include authentication, confidentiality, integrity, communication security and data protection.

The advantages of our planned approach are extending the trusted computing technology to accomplish its requirements for the cloud computing and then fulfil the trusted cloud computing. To integrate these hardware modules with cloud computing system is a difficult work and need more unfathomable study. We develop a model system of trusted cloud computing, which is based on the trusted computing platform. It can provide stretchy security services for users. The Trusted Computing Platform provides cloud computing a sheltered base for achieve trusted computing. We will make the actual design more practical and operational in the imminent. In future, we would also like to study over the impact of more security in this proposed method.

REFERENCES

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

[2] CloudComputing:http://en.wikipedia.org/wiki/Cloud_computing , Accessed: 28/07/2011.

[3] Cloud Computing, http://www.techno-pulse.com/ Cloud Computing for Beginners, Accessed: 28/07/2011.

[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 the18th 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: 28/07/2011.

[16] Trusted computing Technology : http://en.wikipedia.org/wiki/Trusted_Computing. Accessed: 28/07/2011.

[17] Trusted computing : http://www.wave.com. Accessed: 30/07/2011.

[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.

ABOUT AUTHORS

Mr. P.Senthil is currently pursing M.E, CSE in Coimbatore Institute of Engineering and Technology (C.I.E.T), Coimbatore and received his B.Tech degree in Information Technology at Dhanalakshmi Srinivasan Engineering College, Perambalur. His Research areas are Networking and Cloud Computing.

Mr.N.Boopal is working as an Assistant Professor in C.I.E.T, Coimbatore. He received his M.E degree in Computer Science and Engineering at Anna university of Technology, Coimbatore and received B.E CSE in Coimbatore Institute of Engineering and Technology (C.I.E.T), Coimbatore. He has a four and half years of teaching experience. His Research areas are Mobile Cloud Computing and Software Engineering.

Ms R.Vanathi is currently pursing M.E, CSE in Coimbatore Institute of Engineering and Technology (C.I.E.T), Coimbatore and received her B.E Degree in Information Technology at Karunya University, Coimbatore. Her Research areas are Networking and Cloud Computing.