Internet of Things and Cloud Computing
2017; 5(3): 38-43
http://www.sciencepublishinggroup.com/j/iotcc
doi: 10.11648/j.iotcc.20170503.11
ISSN: 2376-7715 (Print); ISSN: 2376-7731 (Online)

Trusted Attestation System for Cloud Computing Environment Using Trusted Platform Module

E. Padma[1, 2], S. Rajalakshmi[1, 2]

[1]Department of CSE, SCSVMV University, Kanchipuram, India
[2]Department of CSA & SJCAC, SCSVMV University, Kanchipuram, India

Email address:
mailtopadma@kanchiuniv.ac.in (E. Padma), rajalakshmi.s@kanchiuniv.ac.in (S. Rajalakshmi)

To cite this article:
E. Padma, S. Rajalakshmi. Trusted Attestation System for Cloud Computing Environment Using Trusted Platform Module. *Internet of Things and Cloud Computing*. Vol. 5, No. 3, 2017, pp. 38-43. doi: 10.11648/j.iotcc.20170503.11

Received: March 21, 2017; **Accepted**: April 18, 2017; **Published**: June 19, 2017

Abstract: In the context of Trusted Attestation System in Cloud Computing Environment the Root of Trust for Attestation plays a vital role for security feature with Trusted Computing. The main aim of trusted attestation process is to provide an effective mechanism for the interconnected public and private systems in a well secured platform using Trusted Platform Module. The mechanism created by the trusted attestation phase gains assurance about data integrity and trustworthiness. The Trusted Attestation System enables the trusted computing functionalities for all authorized users in the current working environment. The Cloud Computing Environment extends the failure rate as attacks on public data and private data for the trusted system. The authenticated integrity state of a trusted system involves the Root of Trust for Attestation (RTA). In the cloud environment an attested user is trusted to behave with the available standard technologies like management of identity, digital signatures, exchange of credential, certificates and management of key. The trusted attestation system in the cloud environment provides Trust as a service (TaaS) for the generation of key. The credential exchange for the trusted environment enhances the facility for Cloud Computing Environment (CCE).

Keywords: Trusted Attestation, Digital Signature, Root of Trust for Attestation, Trustasa Service, Rusted Computing Environment

1. Introduction

Cloud Computing aims at providing dynamic scalability computing resources over the Internet as a Service [5]. With the advent of cloud environment, many users have access to various latest technologies. The cloud system allows better optimization for information technology resources with unlimited bandwidth and greater flexibility at a minimized cost. The system guarantees confidentiality, authenticity, integrity, privacy as well as availability. The attacks on data confidentiality and data integrity enable hackers to thwart the important data.

In this context the trustworthiness of a platform for cloud computing environment is defined and verified with some fundamental and challenging issues. Trusted Computing is a new platform for providing security which has been modeled by the Trusted Computing Group (TCG) [1] based on Trusted Platform Module (TPM) [2]. TPM has been attached to the mother board of computer by having the ability of creation and key storage with the mechanism of cryptography, authentication of identity and storage measurement log. TPM serves as the root of trusted integrity authentication. The TPM signs to guarantee trustworthiness and freshness of characteristics which are needed. It serves as Root of Trust for Attestation (RTA) in Trusted Computing. RTA is for vouching the accuracy of the information and protecting the privacy of the host of the TPM.TCG develops a solution using a trusted attester (Privacy CA) by securing Enhanced Trusted Attestation Key (ETAK) certificated by Privacy CA and signs the message by using TAK. The Trusted Attestation System usage is static and interactive with cloud computing environments.

This paper analyses the existing architecture of cloud services and trusted computing environment with Trust as a Service and gives their limitation. Then trusted approach for the cloud computing environment is presented for Trusted Attestation System which is more secure for attestation of the

users. Attester and Verifier check the authenticity for the attested user. The Root of Trust for Attestation (RTA) is to attest the computing environment more trustworthy.

2. Existing Architecture

2.1. Architecture of Trusted Computing Environment

The Trusted Computing Group provides enormous services for the massive number of system. Distributed System alone deals with Secrecy, Integrity, Availability and Accountability as the model of security. The Secrecy feature deals with controlling accessed information. Integrity deals with the modification of Information. The term Availability prompts access to information and resources. The Accountability service has all accessing right [10] to provide information about the individual user. Authentication, peer-to-peer authentication for communicating entities acts as security information for the concerned user. The distribution demands a communication system between entities. Security messages and secured messages can be transported. The performance is reduced apparently when the cryptographic computing are processed. The challenges of TPM are less performance due to cryptographic computing in distributed system. Also, the distributed computing environment is not enough secured with the creation and protection of certificates [11]. The trusted root is not defined clearly in the distributed computing environment. In this paper the challenges of the exempted performance are defined individually for each user with attestation and verification process.

Table 1. *Classification of trusting various environments.*

Trust in Information System	Trust in Distributed Computing Environment	Trust in Operating System and Application
a)Retrieval of authenticated information	a) Data Integrity for various users.	a)User identification and authentication
b)Trusted Data Access	b)Trust evaluation for secure nodes.	b)Data access control and evaluation of access control
c)Trust Storage Capacity	c)Node cooperation	c)reusable protection mechanism
		d)Audit log file

The challenges for trusted computing environment deals with the services that are controllable, Accessible, dependable etc., The relationship between trust and distrust act as global computing that exist as dynamic interaction and cooperation for end user-to-system, system-to-system, system-to-end user and end user-to-end user [4] .The model of trusted computing need to be identified by the trust implication, distrust and mistrust. Trust as a Service needs to be established for access controlling, management of identity and privacy intrusion for security detection. The reasons used by the cloud users in trusted computing environment for the security policies are very limited. The scope of the security mechanism has to be implemented with the provided TaaS. The attestation tools for various users are to be enhanced with appropriate servers.

2.2. Architecture of TPM

The several specifications published by TCG has various concepts of trusted infrastructures [6] The Trusted Computing Group specifies the TPM as one of the core component The current wide spread feature for implementing the concept of TPM is a small cryptographic chip attached to the main board with the ability of creation and key storage by providing cryptographic mechanisms like RSA, SHA-1, HMAC and functions as digital signing, authenticity of identity and measurement of integrity. The configuration parameters which are in a trusted sequence can be sent as a report for the secure authenticity of each computer. With Reference to figure 1, the augmented Platform boot processes allows the TPM to measure each of the components in the system and securely store the results of the measurements in Platform Configuration Registers(PCR) within the TPM.PCR values are used to identify unsafe configurations at system boot by preventing inadvertent network connection.

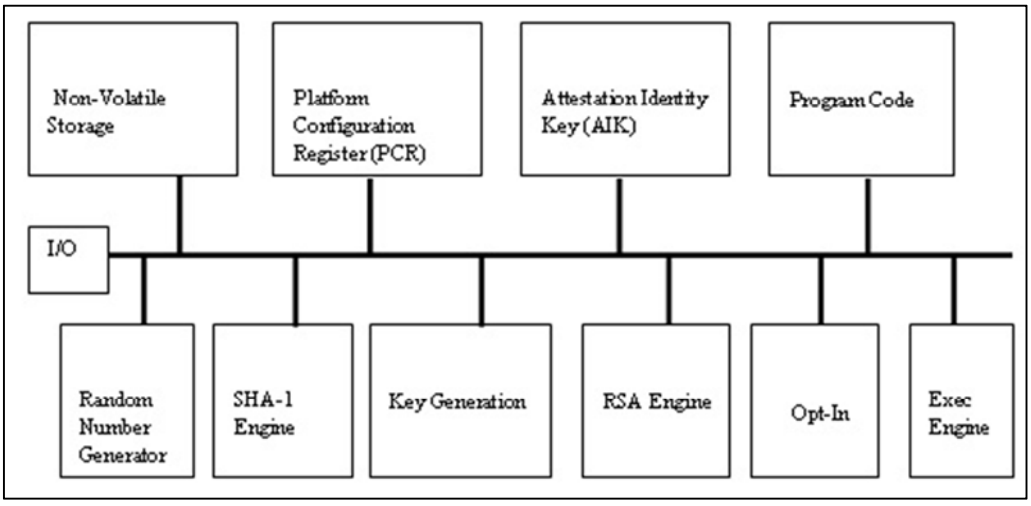

Figure 1. *Architecture of TPM.*

2.3. Various Types of Related Trust

Trust revolves around assurance and confidence for the expected information services which include people, data and entities. The trusting agent delivers only mutually agreed service in a given context for only limited time slot. As per cloud scenario, the trust has been given assurance for hypervisors to isolate and establish trust for guest or hosted virtual machines [8]. In earlier studies the trust and trust models are studied to a greater extent. The characteristics of trust is categorized into various groups, Knowledge; Prognosticate; Benevolence; Integrity [9]. Zhang et al., have classified the following trust functions [12] Capability of an entity's trustworthiness being measured objectively against a universal standard results in objective trust. If the trust being measured depends on an individual's tastes and interest the resulting trust is called subjective trust. Decisions made based on the individual transactions and their results is known as transaction based trust whereas the trust built based on just opinion of the individuals is opinion based trust. If the trust building operation requires information from each and every node, it is called complete information it is known as either global trust function or complete trust function. If the information collected only from neighbor it is called localized information trust function. If the trust worthiness of an entity is ranked from the best to worst, it is rank based trust whereas the trust declared yes or no depending present trust threshold is known as threshold based trust.

3. Proposed Methodology

In the proposed methodology, the Trust as a Service is used to access the data and to maintain the integrity in the cloud environment. The trusted attestation key algorithm plays a role of attesting the authorized user. The identity management for all the users in the cloud environment will be generated using RTA [14]. The generated authenticity will be used by each individual to get grant for exchanging the trusted credentials. The Credential checks for the authorization and then grants the right for accessing the information from the cloud environment. Trust as a Service checks the digital signature for the user and give attestation as a trusted user for accessing the user level information. The algorithm then enters into verification phase by verifying the trusted user by issuing the attested key. In this phase, the signature of the trusted party will be verified using the cryptosystem. The Trusted Attestation System divides the users into two levels i.e., User Level and Machine Level.

With reference to figure 2, the cloud computing environment provides way for use Enhanced Trusted Attestation Key and Root of Trust for Attestation for On Execution Credential.

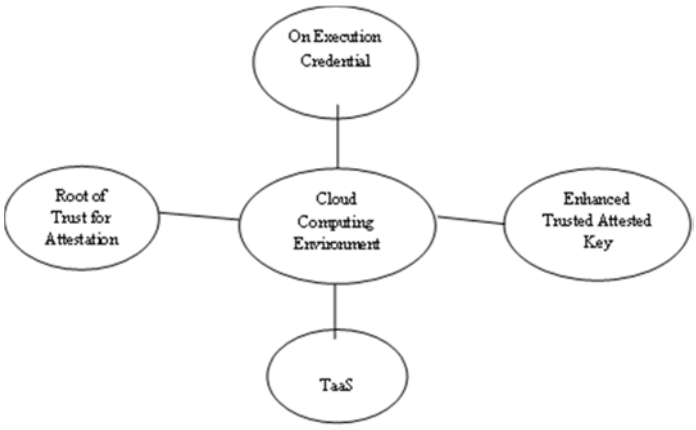

Figure 2. *Process of Cloud Computing Environment.*

3.1. User Level Trusted Attestation Process

In User Level attestation process the key originator has full authorization to use the key as updated key by granting access rights for its entire life time. In User Level scenario, the attestation evidence must be verified by the verifier using attestation protocol [7]. The Credential Manager generates a Certification of Privacy from CA [Attest Cert($TaaS_{pub}$), Attest Sig{ETAK,Nonce} TaaS]. CM issues the certificate to the user to access the information with limited bandwidth.

3.2. Machine Level Trusted Attestation Process

The Machine Level attestation process has full access rights for the usage of keys and machine authentication. The updating of the attestation is not allowed by the individual user. The guarantee issue for the trust process has been issued by the certifying authority CA. The evidence for updating the attestation process using Trust as a Service includes subject key certificate [7]. The Credential Manager generates the certificate request for public users, identity of the user and proof-of-position for private users. CA verifies the usage of accessing keys which are not to be update.

Table 2. *Various Level of Trusted Attestation.*

User Level Trust Attestation	Machine Level Trust Attestation
a)Key originator authorize access rights	a)Individual user not allowed to update keys
b)Limited Bandwidth	b)Use TaaS for requesting key usage

3.3. Attestation for Trusted System

Attestation is the process of giving assurance to the trusted computing environment in a trustworthy manner. The platform is manufactured with a public/private key pair which has been built and incorporated into the hardware. The CA certifies the public part of the key. Each individual platform has a unique hardware key. Using the private part of its hardware key, the system verifies the assertions for trusted computing environment.

In cloud computing environment, the computing systems are interconnected with network as private cloud and public cloud. The verification and authentication phase of the user provide more security using the technique called Trusted Computing [1]. The Trusted Computing as a hardware chip enabled with the security feature has limited exemptions. Trusted Computing in the field of software using the Trusted Attestation will prove the model to be more secure. The verification and attestation key phase provides security for the cloud oriented systems enormously. The Trust as a Service credentials have to be assigned to each individual. Digital Signature provides the facility of sharing diverse resource and coordinated use of available resource in distributed environment. Trusted Attestation Key provides large-scale controlled sharing facility and interoperation among resources that are dispersedly owned and managed. In order to protect the cloud computing system the Trusted Computing Platform (TCP) has to be integrated with Trusted Platform Module (TPM). The TCP can improve the security feature of Execution Environment by providing proper authentication using the Enhanced Trusted Attestation Key with Shared memory space in a large scale. The Authenticity can be matched using Machine Authentication Code. The Authentication code can be generated using the Secure Hashing Key.

With reference to figure 3, the attester waits for Credential Manager to grant permission for trustworthy check to generate TAK.

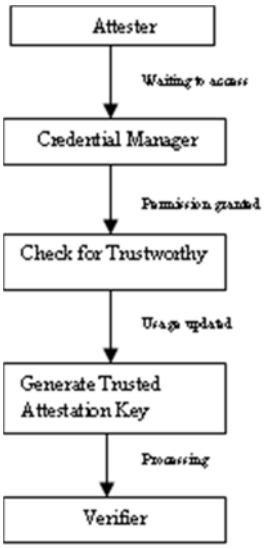

Figure 3. *Role of Credential Manager.*

3.4. Credentials forTrustasa Service

The TCG software authenticates the attested user for trustworthiness. The TCG solution provides authentication for platform in terms of attestation binary values, binding the binary values and seal the binary value. Loosely coupled system is based on the Storage Management Log (SML) for measuring the root of trust to execute code using cryptographic digest [3]. To prove the trustworthiness of an attested system the following two model driven approaches [13] are developed i.e., usage time of trustworthiness and idle time of trustworthiness. The usage approach deals with the used time and arrival time of the attested user. The idle approach deals with the delay time of the attester. The Credential Manager allows the trusted user by using OEC (On-Execution Credential)

On-Execution Credential allows Root of Trust for Attestation for the Cloud Execution Environment. Cloud Execution Environment provides isolated code execution, secure storage and integrity protection of secure execution environment for credential programs [4].

$$RTA_{public}=\text{Sign }\{ETAK\}, SML, TaaS \quad (1)$$

$$RTA_{private}=[\text{Sign }\{ETAK, CA\}, \text{Cert }\{\text{Sign}\{TaaS, CA\}] \quad (2)$$

The above given equation(1) and equation(2) checks Root of Trust for Attestation for both public and private users in the credential phase.

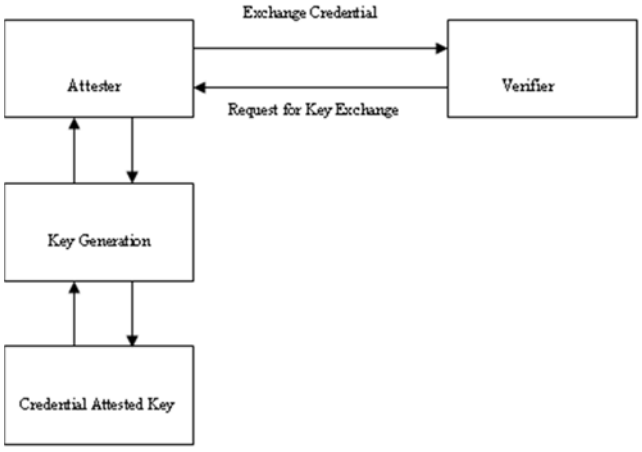

Figure 4. *Process of Attested Credential Key Exchange.*

With reference to the above given Attested Credential Key Exchange figure 4, the symmetric cryptographic algorithm generates a key for attester using TPM key generation function. The Verifier verifies the signature of key K and decrypts it. The key generator function generates Credential Attested Key for the Verifier and sends the key as Credential Exchange through the Attester.

3.5. Enhancement of Trusted Attestation Key

In Cloud Computing Environment, Trusted Attestation Key is attested as Enhanced Trusted Attestation by encrypting the TAK using symmetric cryptographic

algorithm. The request for attestation has been checked by the verifier and grant permission to access the information. The enhancement of Trusted Attestation Key involves the root of trust for attesting the remote users.

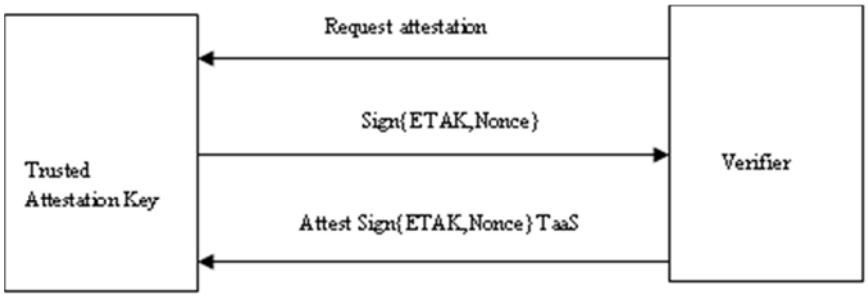

Figure 5. *Process of Trusted Attestation Key.*

Theprocess of ETAK asper figure 5 has the following steps:

Step 1 Verifier : Generate a Nonce(160 bit random number)

Step 2 Verifier-> Trusted Attestation

Step 3 Trusted Attestation -> Verifier{sig{ETAK,Nonce} TaaS,

SML, Cert TaaSpub}

Step 4 Verifier -> Attest Cert(TaaSpub), Attest Sig{ETAK,Nonce} TaaS, Authenticate Nonce & Coherence of SML through ETAK

The Trusted Attested system checks for the platform authentication both for private and public cloud users. The Key can be created by generating the ETAK algorithm [15]. The attested keys can be measured using SML. The identity for each user can be generated with Attestation Identity Key. Then the Credential Manager verifies SML and grant permission for the cloud computing environment.

With reference to below given figure 6, the platform for both public and private cloud users has been explained with Symmetric Cryptography Algorithm, Trusted Attestation Key and Attestation Identity Key with the architectural model of Cloud Computing Environment.

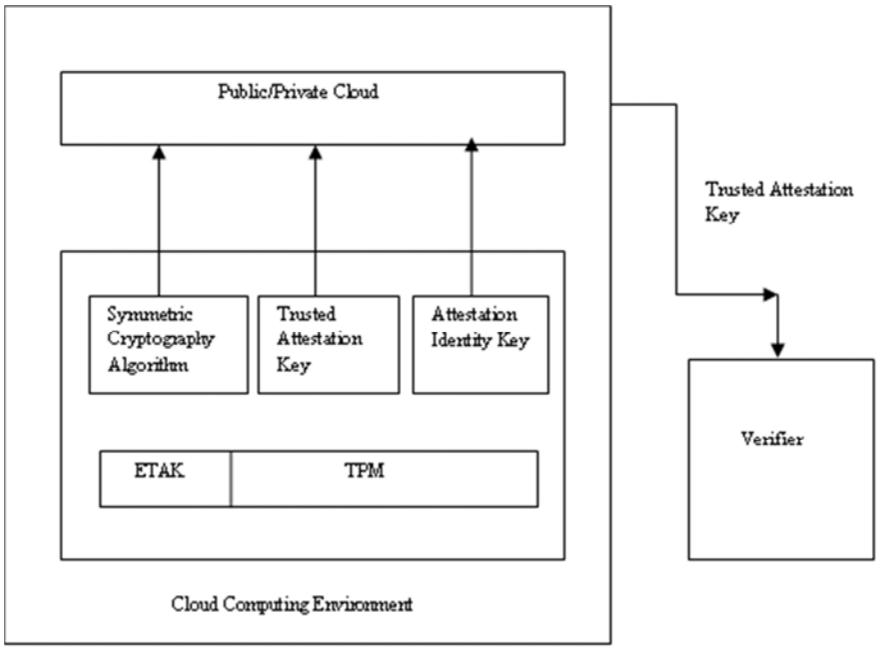

Figure 6. *Architectural Model for Cloud Computing Environment.*

3.6. Trust of Signer and Verifier

The Enhanced Trusted Attestation Key Algorithm deals with the concept of attesting the user with more secure trustworthy manner. The public and private users of ETAK can be provided the double encrypted keys with signing and verifying. The algorithm contains full protection with the process of attestation. The attackers are not easily allowed to attack the system in the cloud computing environment. TaaS enhance the privacy measure to protect the distributed resource. The identification of each and every system has to be accessed with ETAK. The algorithm finds the attacker, who can be signed without authorization. In this phase, the sign of the trusted user will be verified using the cryptosystem. Remote Authentication can be enhanced by using $TaaS_{pub}$ Key. The users count can be managed with buffered log file. Each log file has to be stored

in a separate register called Trust Configuration Register (TCR). The Efficiency of the trust can be calculated using Trust Factor. The buffered log file can be maintained with full trustworthy feature.

4. Conclusion and Future Enhancement

In this paper Enhanced Trusted Attestation Key for Cloud Computing Environment is proposed to overcome the short comes. The trusted attestation involved in the existing system leads to cost orientation, unchangeable and having low performance. In the proposed enhanced trusted attestation process the key generated for credential exchange is more vulnerable. The service provided by the cryptography can be accessed between attester and verifier. The various services available for trusted system make cloud users most safe. However, the TaaS credentials exchange with Root of Trust for Attestation is very difficult to work with Cloud Execution Environment. Also the bandwidth of Trusted Attestation System has to be more secured for the attested user for further extensive application. The future measure can take care of the above two drawbacks.

References

[1] The Trusted Computing Group. Retrieved from http://www.trusted computing group.org.

[2] TCG, TCG TPM Specification Version1.2 Revision103, Retrieved from https://www.trusted computing group.org/specs/TPM.

[3] Xing Huangand Yuxing Peng "An Effective Approach for Remote Attestation in Trusted Computing Proceeding sofInternational Symposium on Web Information Systems and Application" May 22- 242009.

[4] Udhayakumar Shanmugam, Latha Tamilselvan, Uma Nandhini and Dhinakaran "Attestation for Trusted Computing to Assure Security in Cloud Deployment Services International Journal of Information and Electronics Engineering", Vol.2, No.4, July2012.

[5] Mr. Ravindra K. Gupta, Mr. Rajat Pali, Dr. Shailendra Singh, Mr. Gajendra Singh, Mr. Ashutoshk. Dubey "A Comparison with Property Based Resource Attestation to Secure Cloud Environment" CS & IT-CSCP2012. Pp.319–330, 2012.

[6] Trusted Platform Module (TPM) Specifications Retrieved from https://www.truste computing group.org/specs/TPM.

[7] TCG Infrastructure Workgroup Subject Key Attestation Evidence Extension, Specification Version1.0 Revision7 June2005.

[8] S. Udhayakumar, S. Chandrasekar, L. Tamilselvanan and F.Ahmed, "An Adaptive Trust Model for software service sin Hybrid cloud Environment," Proc.15 WSEAS conference on Systems, Recent Researches in Computer Science, 2011, pp.493-502.

[9] D. Harrison McKnight and NormanL. Chervany, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model," in 34th Hawaii International Conference on System Sciences, Island of Maui, HI, USA, 2001.

[10] Claus Fritzner, Leif Nilsen Andsmund Skomedal, "Protecting Security Information in Distributed Systems", GH29 868\91/0000/0245$01.00@1991 IEEE.

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

[12] Q. Zhang, T. Yu, and K. Irwin, "A Classification Scheme for Trust Functions in Reputation-Based Trust Management", in International Workshop on Trust, Security and Reputation on the Semantic Web, Hiroshima, Japan, 2004.

[13] Liang Gu, Xuhua Ding, Robert H. Deng, Yanzhen Zou, Bing Xie, Weizhong Shao, Hong Mei, Model–Driven "Remote Attestation: Attesting Remote System from Behavioral Aspect". The 9th International Conference for Young Computer Scientists, Zhangjiajie, China, November18, 2008.

[14] E. Padma, Dr. S. Rajalakshmi "The Privacy Feature of Trusted Computing Technology using the Concept of Direct A nonymous Attestation with Cloud as a Technique" International Journal of Computer Engineering and Technology (IJCET), ISSN 0976-6367(Print), ISSN0976-6375(Online) Volume 5, Issue 2, February 2014. Pp140-144.

[15] E. Padma, Dr. S. Rajalakshmi "An Effective Approach for Trusted Attestation Key in Distributed Computing Environmen tusing TPM" International Journal of Applied Engineering Research (IJAER), ISSN0973-4562 Volume 9, Number 22 (2014) pp12087-12096.

Biography

E. Padma, Research Scholar, SCSVMV University, Enathur, Tamilnadu, India. Her work experience includes more than 10 years. Area of Specialization is Network Security. Her publication includes "The Privacy Feature of Trusted Computing Technology using the Concept of Direct Anonymous Attestation with Cloud as a Technique" International Journal of Computer Engineering and Technology(IJCET), ISSN0976-6367(Print), ISSN 0976-6375(Online) Volume 5, Issue 2, February 2014, "An Effective Approach for Trusted Attestation Key in Distributed Computing Environment using TPM" International Journal of Applied Engineering Research(IJAER), ISSN0973-4562, Volume 9, Number 22(2014)etc.

S. Rajalakshmi working as Head, Dept. of CSA and Director, SJCAC, SCSVMV University, Enathur, Tamilnadu, India. Her work experience includes more than 15 years. Her area of specialization is Network Security. Her publication includes "Identity Based Encryption Using mRSA in data transfer through VPN", IEE Explore, Volume, Issue, Nov 2006, Pages1-6, "Analysis of Quality of Service using Distributed Coordination function" in AodvJ European Journal of Scientific Research Vol. 58 No1.(2011), pp.6-10, ISSN1450-216Xetc