Trusted platform module based user attestation architecture for cloud infrastructure

PRAMOD [#1], **Dr. B R PRASAD BABU** [*2]

[# 1] Associate Professor, CSE Department, EPCET, VTU, PhD Research Scholar
Bangalore, INDIA

[# 2] Professor & Head, CSE Department, EPCET,
Bangalore, INDIA

[1] pramod741230@gmail.com

[2] brprasadbabu@gmail.com

Abstract- **Cloud computing is s major shift in the IT industry. Many Research topics indicate that the cloud computing industry is substantial and growing rapidly. Numerous technologies have been developed, and now there are many ways to virtualizes IT systems and to get the needed applications on the Internet, through web based applications. Cloud users now can avail their data any time and at any place with Cloud Storage service. With all various benefits of cloud computing, security is always a major concern. Despite the fact that the cloud computing gives getting to the information put away in distributed storage in an adaptable and versatile way, the primary test it countenances is with the security issues. Thus cloud user may think cloud in not secure, because the encryption keys are completely managed by the software; hence there is no attestation on the integrity of client software. The cloud users who needs to send in the dependable and secure environment ought to be affirmed from the Infrastructure as a Service (IaaS) that it has not been corrupted by mischievous acts. Thus, the traditional user identification such as user ID and password can be easily compromised. Besides from the traditional network security solutions, (TCG) trusted computing technology is combined into cloud computing environment to make ensure that the integrity key of platform and offer attestation mechanism for trustworthy services. Thus, enhance the confidence of the IaaS provider. The cryptographic convention received by the Trusted Computing Group empowers the remote confirmation which protects the security of the user in view of the trusted stage. Hence we propose a structure which characterizes Trusted Platform Module (TPM), a trusted registering bunch which demonstrates the protected information access control in the cloud storage with enhance security. In this paper, we define the TPM-enabled key management, remote user attestation and a secure sharing of key across multiple users. We also study various challenges with the current TPM based attestation based techniques. The Portable TPM which is proposed in this paper is not embedded to VMS (Virtual Machines) in order to offer efficiency to the cloud users. Utilizing this methodology, security of the user is taken care in efficient way. We demonstrate proposed scheme effectiveness and efficiency, through extensive experimental evaluation on the live Microsoft Windows Azure platform.**

Keyword: TPM, IaaS, vTPM, cTPM, SMRR, SMM, TCG, TED, DRTM, VLR, DRTM, CA.

I. INTRODUCTION

Cloud computing is the modern era of computing. Industry experts believe that cloud computing as a new technology trend to grow rapidly. Cost is the biggest driver for its expected growth. According to Gartner Inc., cloud computing is a disruptive phenomenon, with the potential to make organizations more responsive. Cloud computing brings out economic advantages such as agility, agility, flexibility, elasticity and innovation. Cloud computing is an web-based facility to share resources such as digital information and software as needed. The main advantage of cloud computing can save a lot of cost on infrastructure and pay-as-you-use model can also be offered through the cloud computing solutions. The above mention features can help small enterprise and mid-sized enterprises to decrease their operational costs. IDC India lead analyst (software and services research), Kamal Vohra stated, “The most attractive feature of this new technology, cloud is the prospect of converting giant, upfront capital investments in Information Technology infrastructure into small, manageable ‘pay-per-use’ annuity payments.”

The Recent IDC cloud research shows that spending cost on public IT cloud services will reach $58.4 billion in 2015 and is expected to be grow more than $107 billion in 2017. Over the year 2013–2017 forecast period, public IT services for the cloud will have a compound annual growth rate (CAGR) of 23.5%, which five times that of the industry overall. Software as a service (SaaS) will always remain the largest public IT cloud services category, which captures 59.7% of revenues in 2017. IDC predicts that by 2017, 80% of new cloud apps will be hosted on six Platform as a Service. Armonk, N.Y. May 2014 announced businesses across the US have ranked IBM the number 1 cloud computing provider, according to an IDC survey of US market preferences for infrastructure-as-a-service (IaaS). Enterprises ranked Amazon 7th, behind Google (5th) and Microsoft (6th). The rankings mentioned above are based on responses from more than four hundred US-based companies. The major Cloud computing services fall into three categories-such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software-as-a-Service (SaaS). The software applications which are deployed from the cloud infrastructure provided by the cloud providers are accessed by the Software-as-a-Service (SaaS).The cloud providers manage and control the cloud application so that the user no need to own the software but rather pay for its use through a web. Platform as a Service (PaaS) which lets the cloud users to deploy their applications on the cloud provider's infrastructure using programming languages and tools supported by the provider. Finally, Infrastructure as a Service (IaaS) authorizes the deployment and the execution of an environment fully controlled by the cloud user, typically a Virtual Machine (VM) – on the Cloud resources. Typically scenario, the user must purchase the infrastructure such as software, data resource, server, network accessories in order to operate. But here, the cloud user can directly purchase all these resources in form of outsourced services from directly from the cloud on "pay-as-you-use" basis. Thus, providing efficiency of services. Here, we mainly focus on the security aspects of the third category of cloud services, i.e., IaaS platforms and more precisely on confidentiality and integrity issues. The security issue arises when the cloud user has to preserve the data confidential on the shared platform. Also, once it is deployed, care must be taken; the integrity of the environment is not corrupted or compromised by the mischievous acts.

An Ideal approach to protect Infrastructure as a Service platforms which based on the approach established from the Trusted Computing Group (TCG) which offer a secure and protective environment with the hardware device called the Trusted Platform Module (TPM). TPM designates both the name of a specification detailing a secure crypto processor as well as the implementation of that specification, often called the TPM chip. In [5], it proposes DFCloud, a secure way to access data control method of cloud storage services to handle these problems found in the typical cloud storage service. Drop box TPM which asserts the virtue of remote authentication and gets interacted with the symmetric key which can be used for various cryptographic purposes, from the protection of network communications to data encryption. The SMRAM need to setup properly by the BIOS at boot time and to remain tamper-proof from cache poisoning attacks as in [7].In the IaaS context, it ensures that only the resource which is available in remote with which the cloud user is communicating using the TCG protocol can interact with the encrypted data. Farazi Sabhai et. al. [2] discusses the well-known Gartner's seven security issues. A TPM is a small tamper proof enabled hardware chip embedded in most recent motherboards.

Zhidong et. al. [6] address the cloud computing security challenges by proposing a solution called the Trusted Computing Platform (TCP). This paper presents portable TPM, an extension of the TCG's model which offers an additional secret key to the TPM and shares the key with the cloud environment. Therefore, with this, the cloud environment can not only create and share the secret keys of TPM and data over multiple platforms which belong to a single cloud user. Recent advances in automatic protocol analysis tools [4] allow to enhance the attack complexity against the analysed protocol and detect design errors. This [8] proposes a new TPM enabled password caching and verification method called PwdCaVe. In this [10], it address the issues by incorporating a hardware-based Trusted Platform Module (TPM) mechanism called the Trusted Extension Device (TED) together with the security model and protocol to allow stronger privacy of data compared to software-based security protocols.

Proposed System

Consider a scenario where a cloud user, cloud provider, a blacklisting controller and the cloud verifiers are concerned. Issuing of membership certificates done by Cloud Provider to the cloud users. The certificate of membership is blacklisted by the blacklisting controller. The cloud users in the system may vary and also users may access data according to their individual need. [1] Presents cTPM, an extension of the TPM's design which comes with an additional root key to the TPM and shares that root key with the cloud. The paper [3] presents secure way of auditing scheme for cloud computing systems. Let us consider hardware based authentication key in an ideal system. The various operations carried out by the authentication key k are initialization, registering, taking membership approval and finally blacklisting.

In initialize phase, controller control every entity, which is indicated by the authentication key K. Initially cloud users are needed to register. A cloud user requests to the authenticator with key 𝕂 and the authenticator replies to the cloud provider whether the cloud user can complete registration process or not. If the cloud provider approves, the authenticator informs the cloud user that he can become a member. In the approval for membership phase, the authenticator sends a request that he wants to contact the verifier. With, it informs the verifier that user wants to perform the membership approval without revealing to the verifier who the authenticator is. The verifier then chooses a message s and sends this message s to the authenticator. If the authenticator is not a member then aborts. Otherwise, tells the authenticator whether he has been blacklisted and asks him whether to proceed. If the authenticator does not abort then, $\mathbb{K}$ lets the verifier know that a user has been blacklisted signed the message s. Otherwise, $\mathbb{K}$ which informs the verifier that message s has been signed by a legitimate member. Blacklist revokes the membership authentication. The blacklisting controller tells the authenticator to blacklist a user. If the cloud user is not a group member, denies the request. Otherwise, $\mathbb{K}$ marks the cloud user as blacklisted.

A cloud user who is not a member or is a member but has been blacklisted cannot succeed in membership approval to any verifiers. The verifiers not able identify who is authenticator in a membership approval process, thus proving anonymity of verifier. In ideal system, Blacklist causes verifiers to reject message s signed by a blacklisted cloud user. In proposed protocol, if user's private key is compromised and the cloud user is blacklisted, then the signatures from this blacklisted user become linkable to an honest verifier.

As a result, blacklisted users who might reveal their private keys deliberately lose their privacy are blacklisted. Thus, an authenticator can check whether the user has been blacklisted from on the blacklist, before the user signs a signature and sends it to the verifier. If the authenticator had a knowledge about the cloud user has been blacklisted, then cloud user not proceed. Proposed scheme security relies on the public key cryptographic protocol and the Diffie-Hellman assumption. The cryptographic protocol based on public key is established as follows. It is computationally infeasible, on input of a random modulus M and a random element M and random element $a \in$ compute value > 1 and q such that $qi \equiv (mod\ M)$. In other words, for every probabilistic polynomial-time algorithm R.

$$\begin{aligned}\mathcal{B}[M \leftarrow \mathcal{K}(1^p), a \in \mathbb{A}_l^*, (q,i) \leftarrow R(M,a) : q^i \\ \equiv a(mod\ M) \wedge 1 < i < M] \\ = \phi(p)\end{aligned}$$

Where $\mathcal{K}(1^p)$ is an algorithm that generates a public key modulus and $\phi(p)$ is a negligible function. Let u be an lu bit prime and v is an lv-bit prime such that $u - 1$. Let $s \in \mathbb{A}u$ be a random element of order v. Then, for sufficiently large values of lu and lv, the distribution $\{(sx,sy,sz)\}$ is computationally indistinguishable from the distribution {(sx,sy,sxy)}, where x,y and z $z$are random elements from $\mathbb{A}u$. It can be formally stated as, for every probabilistic polynomial-time algorithm R, Diffie-Hellman assumption is given by:

$|\mathrm{B}[R(u,v,s,sx,sy,sxy) = 1] - \mathrm{B}[R(u,v,s,sx,sy,sz) = 1]| = \phi(p)$.

Where $\phi(p)$ a negligible function and the probabilities is are taken over the choice of u,v,s according to some generation function $\mathcal{K}(1^p)$ and the random choice of x,y and z in $\mathbb{A}u$. Remote authentication of the hardware based authentication key is enabled in the cryptographic protocols. Here, it preserves the privacy of the cloud user which contains the key $\mathbb{K}$.

This above mentioned protocol comprises of the cloud provider, authenticator who provides access issued by the cloud provider and the verifier who validates with the authenticator. The authenticator consists of the portable key k which preserves the privacy for the cloud user. The protocol is constructed by the Camenisch- Lysyanskaya signature scheme, where it has two secret messages m_0 and m_1, and attains the CL signature (membership of the user) on m_0 and m_1 from the cloud provider through a secure protocol, and thus the user is verified by the verifier. Here, the authenticator chooses two random lm -bit secret messages m_0 and m_1, then

interacts with the cloud provider, and in the end obtains (R, i, q) from the protocol such that $\mathrm{R}^{\mathrm{i}}\mathrm{G}^{\mathrm{m0}}\mathrm{G}^{\mathrm{m1}}\mathrm{Q}^{\mathrm{q}} \equiv$ A(mod M).The authenticator will check with verifier that the user is verified and possess the CL-signature on the values of m_0 and m_1.

This can be done by values $(m\ ,m\ ,R,i,q\ )$ such that $RiGm0Gm1Qq \equiv A(mod\ M)$ .Let $m = m0 + m1$ the authenticator also computes $P := \mathcal{D}m\ mod\ u$ where $\mathcal{D}$ is a generator of an algebra group where computing discrete logarithms is infeasible, and proves to the verifier that the exponent m is related to $m0$ and $m1$.

This protocol choose $\mathcal{D}$ the value of $\mathcal{D}$ need to be chosen randomly by the authenticator, or can be derived from the verifier's name by using an appropriate hash function. If authentication key $\mathbb{K}$ was found comprised and its private key, $m0$, $m1$, was compromised, the values $m0$ and $m1$ are extracted and put on a blacklist. The verifier can then check the public key P in the signature against this blacklist by comparing it with $\mathcal{D}m0$+$m12lm$ for all pair's $m0$ and $m1$ on the black list.

In our scheme, there are various types of entities exists such as blacklisting controller ,cloud users and verifiers. The cloud provider, blacklisting controller could be the same entity or separate entities. Proposed scheme based on cryptographic scheme and uses the Camenisch Lysyanskaya(CL) signature scheme as underlying building block. To simplify our work, we modified the cryptographic protocol scheme in the following ways: 1) each cloud user chooses a single secret m instead of two secrets, and 2) the signature operation is performed solely by the cloud user (along with authentication key), instead of split by two separate entities(authentication key $\mathbb{K}$ and host in the cryptographic protocol scheme).

In the register phase, cloud user chooses a secret message m and sends to cloud provider a commitment to m, i.e., $C := GmQq'$ where q' is a value chosen randomly by the cloud user. Also, the cloud user computes $P := \mathcal{D}m\ mod\ u$, where $\mathcal{D}I$ is a number derived from the cloud provider's base name. The user sends P to the provider. The cloud provider then issues a membership for the cloud user based on C. The cloud provider chooses a random integer q'' and a random prime number i, then computes R such that $RiCQq'' \equiv (mod\ M)$, and sends the user (R,q''). The cloud provider also proves to the user that he computed R correctly. The CL signature on m is then $R := q' + q''$. The cloud users private key is set to be (R).

A cloud user can now prove that he is a valid member not a member by proving that user has a CL signature on the value m. This can be done by values of m and q such that $RiGmQq \equiv A\ (mod\ M)$. Also, the cloud user computes $P := \mathcal{D}m\ mod\ u$ where $\mathcal{D}$ is a random base picked up by the user, reveals $\mathcal{D}$ and P , and proves that $\log\mathcal{D}^{P}$ is the same as the one in his private key. The value P is used for same purposed of blacklist. As in the cryptographic scheme, if a user's private key (R,i,m,q) is compromised and gets exposed to the public, m is put in the blacklist.

The verifier can then check and verifies P in the signature against the blacklist by comparing it with $\mathcal{D}m$ for all ̂in the blacklist. This type of blacklist is called as private key-based blacklist and use $Vpriv$ to denote the blacklist of this type.

This scheme supports two blacklist methods, one is signature based blacklist and the other is cloud provider-based blacklist. In signature based blacklist, suppose a verifier received a signature from an authenticator and then decided that the authenticator was compromised. The verifier reports the signature to the blacklisting controller who later places ($\mathcal{D}$,) of the signature to the signature-based blacklist, Where $\log\mathcal{D}^{P}$ is the secret of the compromised authenticator. To prove membership, a user with private key (R,) now needs not only to prove the (R,,m,q) such that $RiCQq'' \equiv A(mod\ M)$. But also to prove that m in his private key is different from $\log\mathcal{D}^{P}$ for each ($\mathcal{D}$,) pair in the signature-based blacklist. We use $Vign$ to denote the blacklist of this type. In the cloud provider-based blacklist, the provider obtained (P,) from a user when the user registers and later decided to revoke this user from some reason. The cloud provider sends (P) to the blacklisting controller who places P to the cloud provider-based blacklist, where $\log\mathcal{D}I^{P}$ is the secret of the blacklisted user. To prove the membership of the user, a user needs to prove that m in his/her private key is different from $\log\mathcal{D}I$ for each P in the cloud provider-based blacklist. We use cloud provider Vp to denote the blacklist of this type.

A. Membership approval for Resource constrained devices

The resource-constrained device, such as a TPM, a smart card, or a secure coprocessor can be used as authenticator; it can facilitate the part of the signing operation to a semi trusted host. Essentially, the signing operation is partitioned between a computationally weak device (denoted as the principal authenticator) and a resource abundant but less-trusted host. Observe that if the host does not cooperate, then it is a denial of service. Thus, the host platform is trusted for performing its portion of computation correctly. However, the host is not allowed to learn the private key of the authenticator or to forge a signature without the principal authenticator's involvement. This model is used in the original cryptographic protocol scheme with a concrete security model.

B. Using TPM Hardware

We have the following benefits using the TPM hardware: 1) less computational work, 2) portable and 3) trusted blacklist mechanism. The main design principle is that the host system and the hardware together perform the membership approval as the authenticator. The host, if compromised, would break the anonymity of the user but not able come to know the user's membership private key. Because, the host can pad some identifier to each message sent by the hardware device. Major advantage of using trusted hardware device is to have more blacklisting is efficient.

Thus, a cloud user is blacklisted in the following cases. The user's membership private key was deleted from the trusted hardware device, and was published widely so that everyone knows this compromised private key, it's been blacklisted. When the user's membership private key was extracted from the trusted hardware device by the adversary. The cloud provider suspects that the cloud user's hardware device was compromised, but has not obtained the user's private key. Thus, blacklisted. The user's membership private key was extracted from the hardware device by the adversary. The blacklisting controller suspects that the hardware device was corrupted.

The blacklisting controller obtains a signature from the corrupted device but has not obtained the private key becomes blacklisted. The cloud provider blacklists the user for some management reason, e.g., the user's membership expired. The user is blacklisted from transactions; more specifically the user abuses his group privilege and is blacklisted by the blacklisting controller after the user conducted a membership approval.

II. RESULTS

We mainly aim on data leakages that might occur in the cloud environment. Hardware based Portable TPM attestation architecture supports hardware-based key management by using TPM devices to provide better security and hence device portability is achieved. Therefore, a cloud user who access content of cloud storage in secure environment and securely store cloud user data to the remote cloud server using portable devices which provides additional security.

The proposed system has been simulated on live Microsoft Windows Azure public cloud environment for various performance parameters such as memory utilization, user attestation overhead and the *Q*OS perspective for CPU utilization. The relative study for these all factors has been demonstrated . This system or model performance has been verified for various user sizes with the assigned authentication hardware devices and the effectiveness as well as performance parameters have been verified for its robustness justification.

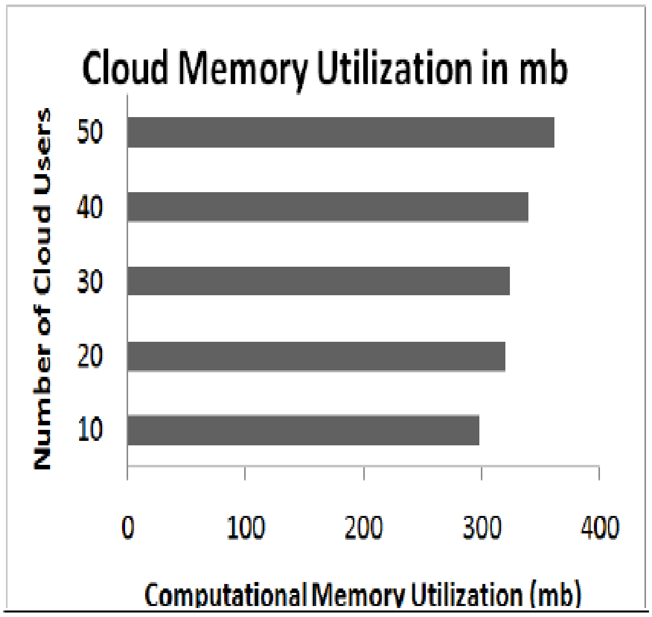

Figure 1: Cloud Memory Utilization

The above mentioned figure (Figure 1) shows the cloud memory utilization in megabytes (MB) based on the respective set of cloud users from 10 to 50. Here, the memory utilization is computed based on the cloud user which is able to access the cloud service through credentials along with the additional authenticated device, TPM. Usually for cloud users to access cloud, cloud providers may be concerned about the memory utilization of varied number of users. From the graph, it can be justified that less memory is utilization with the additional security parameter. It clearly shows that even if we increased the number of cloud users are 50, there is negligible changes in cloud memory utilization. Thus, memory computation show in graph is highly adaptive.

Based on the simulated data, the graph (Figure 2) is plotted making the comparison of the user attestation overhead of our proposed system with portable based TPM device against the cloud user attestation without TPM. The computation overheads computed in presence and absence of TPM [12] is being evaluated in milliseconds(ms). Without the external device it is obvious that the computation is of less value. Therefore, from the figure it is evaluated that the average computation overhead without the TPM device (without added security) is 5.58ms. The average computation overhead with the usage of TPM which provides additional security is evaluated to be 6.35ms. Thus, the average computational overhead increase is which is very negligible when considering a highly secure cloud environment with the cryptographic protocols.

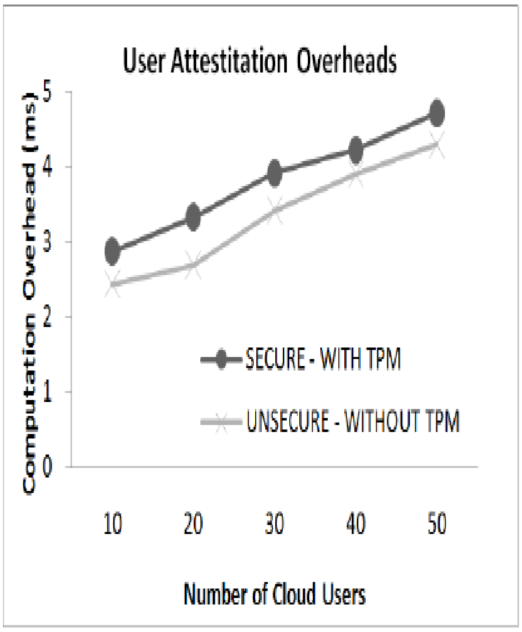

Figure 2: User Attestation Overhead

III.CONCLUSION

In particular, the challenges of preserving confidentiality and securing the cloud data and also the need to maintain the credentials while preserving the policies set out by the cloud provider. The proposed work mainly aims on data leakages that might occur at client-side or server-side [11]. Property based attestation techniques for the cloud is proposed in this paper. We have designed a Portable TPM based device, for further security. We propose a portable device which is used in the authentication and verification of the cloud user. We have highlighted that our secure data sharing protocol, which allows highly confidential data sharing. The portable TPM based user attestation architecture for cloud environments model exploits client-side authentication with encryption technique to mitigate server-side data leakages such as malicious insider attack or exploiting vulnerabilities of server platform. Due to remote attestation protocol for verifying the cloud user, we ensure that malicious behaviors will not occur.

REFERENCES

1. Benoit Bertholon, Sebastien Varrette and Pascal Bouvry, “CERTICLOUD: a Novel TPM-based Approach to Ensure Cloud IaaS Security” 2011.
2. Farzad Sabahi, ”Cloud Computing Security Threats and Responses”, IEEE 3488 rd International Conference on Communication software and Networks(ICCSN), 27-29 May 2011,pp 245-249, Print ISBN: 978-1-61284-485-5, DOI: 10.1109/ICCSN.2011.6014715
3. Houlihan, R.; Xiaojiang Du, "An effective auditing scheme for cloud computing," *Global Communications Conference (GLOBECOM), 2012 IEEE* , vol., no., pp.1599,1604, 3-7 Dec. 2012
4. xin Wan; Zhiting Xiao; Yi Ren, "Building Trust into Cloud Computing Using Virtualization of TPM," Multimedia Information Networking and Security (MINES), 2012.
5. Jaebok Shin; Yungu Kim; Wooram Park; Chanik Park, "DFCloud: A TPM-based secure data access control method of cloud storage in mobile devices," *Cloud Computing Technology Conference on* , vol., no., pp.551,556, 3-6 Dec. 2012
6. Zhidong Shen, Qiang Tong “ The Security of Cloud Computing System enabled by Trusted Computing Technology”, 2 International Conference on Signal Processing Systems Print ISBN: 978-1-4244-6892-8, DOI: 10.1109/ICSPS.2010.5555234.
7. Duflot "Getting into the SMRAM: SMM reloaded" Proc. of the 10th CanSecWest conference, 2009.
8. Hua Wang; Yao Guo; Xia Zhao; Xiangqun Chen, "Keep Passwords Away from Memory: Password Caching and Verification Using TPM," Advanced Information Networking and Applications, 2008. AINA 2008. 22nd International Conference on ,
vol., no., pp.755,762, 25-28 March 2008

AUTHOR PROFILE

Mr. PRAMOD, Working as Associate Professor, CSE department, EPCET. Published various journals in resource management in Cloud computing and Usage of TPM for Securing Cloud Services.

Dr. B R PRASAD BABU, working as Professor & Head, CSE Department, EPCET. His research topics are Ad Hoc networks, Mobile communication, Software engineering. He had published more than 50 National and International Journals. Currently guiding PhD Research Scholars at Visvesvaraya technological university and Jawaharlal technological university.