ISSN (e): 2250 – 3005 || Volume, 08 || Issue, 8|| August – 2018 ||
International Journal of Computational Engineering Research (IJCER)

Securing SaaS Cloud Infrastructure Using Portable TPM

Dr. Pramod [1], Dr. Sunitha B S [2]
1 *Associate Professor, CSE Dept, PESITM, Shivamogga,*
2 Associate Professor, ISE Dept, PESITM, Shivamogga,
Corresponding Author: Dr. Pramod

ABSTRACT
Cloud computing is a model ,which can enable network on global demand or the ability to access of network to a distributed pool of configurable resources such as applications, storage and services. These resources are available with minimal management efforts and also provisioned by the cloud service providers. SaaS is software model the users can access the applications that is owned, delivered and managed remotely by providers. Cost saving is the key benefit of using SaaS in the enterprises as to save the hardware, or physical storage. However, based on data sharing properties, these may be vulnerable to malicious attacks. Thus, with the user credentials it can be easily compromised and the services of SaaS are accessed. The services can be acquired even by the URLs when compromised. To address and guarantee secure remote attestation for cloud service access, this paper presented a novel technique Securing SaaS Cloud Infrastructure using Trusted Platform Module (TPM) based provisioning. A portable TPM is used for accessing SaaS which provides better security. A remote authentication can be done by the use of cryptographic techniques which is used to preserve the privacy of user and it is modelled as TPM. TPM is used for strong user authentication framework apart from user credentials and it demonstrates the secured data access control in the cloud storage space by offering additional security.
KEYWORDS: PaaS, IaaS, SaaS, TPM, TCG

Date of Submission: 27-07-2018 Date of acceptance: 11-08-2018

I. INTRODUCTION

Cloud computing is a model which enables the service as on demand of the user. Services are distributed pool of configurable resources in particular server, storage and network .These types of services are provisioned and maintained by the various service providers in the network with negligible endeavor or interaction. Cloud computing adopts the"pay and use"; it reduced the computation cost in the IT industries. Cloud services are available on demand of the user. User of cloud only pay as per use basis on the utilization of the service, how much they utilized that much of amount only they will pay. It is similar like paying the electricity bill, how much electricity is consuming user will pay for that only. Therefore cloud computing also known as the utility computing. Symbol to represent the internet is cloud from that cloud computing name is inspired because in cloud computing everything handled over the internet. As cloud represent the collection of computers and servers which is accessible by the users over the internet. These computers and servers are managed by a third party in various locations. Multiple numbers of operating systems can be run by these machines. Hosted services are offered through the cloud-computing to its client by making use of internet. Three cloud computing services are categorized as IaaS (Infrastructure-as-a-Service), SaaS (Software-as-a-Service) and PaaS (Platform-as-a-Service). In Infrastructure-as-a-Service ,Cloud-service-providers give the virtual server and various services to its client. Virtual server is configured by the clients with its provided storage assigned by the service providers example of it is Amazon's EC2. In Platform-as-a-Service, over the internet cloud-service-providers gives the flexibility to their clients for building their application/software on the providers platform, example is Google App Engine. In Software-as-a-Service, client of cloud-computing can use the various applications. As per need or as long as it is required and pay the amount for that software based on time. Example of SaaS application is the Gmail, Salesforce.com and MapQuest.

II. LITERATURE SURVEY

The pattern towards Cloud processing framework [4] has expanded the requirement for new techniques that permit information proprietors to impart their information to others safely taking into account the necessities of various partners. The information proprietor should have the capacity to share secret information while appointing a considerable part of the importance of access-control administration to the Cloud as well as trusted endeavors. The shortage of such techniques to improve protection and also protection might ruin the development of distributed computing. In particular, there is actually a developing require to much enhanced control security-keys of information take place in the cloud. BYOD brings an initial step towards empowering secure and productive key administration, generally be that as it may possibly, the information owner can't promise that the information purchaser's device by itself is secure

Cloud computing appears to be the upcoming technology of IT solutions [5]. It also allows the user to send their application program software and data to the network which is dissimilar from the conventional solutions. Due to the fact of this IT services are not inside the physical, logical, users manages, it progressed up using novel distinct security challenges. Certainly one of the vital one is making sure of data storage security. The associate network infrastructure for cloud data storage space constitute a third party examiner which manage to pay for trusting verification for consumer to operate their information in cloud. The concerns of data storage space security in cloud-computing is examined in this paper. A new third-party auditor type is offered in this paper. The evident advantage of proposed approach is the cloud-service-provider can provide the functions which were offered by the old third- party-auditor and make it trustworthy. Hence it indeed minimizes the difficulty in cloud-computing.

In software as a service model [6] now a days Biometric Authentication is new demand used for the strong authentication in the web based environment. While adoption of both the biometric technologies and the SaaS system negatively associated with the perceived security and data protection risks. Here author used various evaluation criteria for the Bio SaaS system and also it include both the point for security Biometric and SaaS. Author also apply the prototypical implementation pertaining to a SaaS-compliant biometric authentication services which is actually is dependent upon the keystroke and the dynamic organization deployment.

Client of Cloud computing environment [7] can be access a software service over the internet which is available on demand of the client and this service known as SaaS. Huge amount of SaaS infrastructures are available over the internet and these all are sharing in nature. Due to sharing in nature SaaS application easily targetable by the malicious attack. Here author introduces an IntTest a versatile and successful coordination confirmation stage for the SaaS clouds. IntTest offers another incorporated validation diagram examination approach that can offer more grounded aggressor stick directing force than prior approach. Here author exhibited a model of the IntTest-framework and confirmed it on a generation cloud-computing foundation on IBM System on the S stream preparing applications. Through the trial result, author demonstrates that the through the IntTest-approach higher exactness can be accomplished in the event of aggressor pinpointing case. IntTest-approach not required any special hardware so this is also a cost effective approach.

Table 1: Security Monitoring for Cloud Service[1]

	SaaS	PaaS	IaaS
Application monitoring	Allow	Monitor application logs for vulnerabilities (may be available via the PaaS platform)	Monitor application vulnerabilities (OWASP Top 10) and application event logs for intrusions
Network monitoring	Allow	Provider responsibility	Monitor the network interfaces of virtual instances
Database monitoring	Allow	Provider responsibility	Install database security monitoring tool on VMs hosting database and log events to a dedicated and persistent log server
Host monitoring	Allow	Provider responsibility	Monitor security events from host IDSs such as OSSEC Log events to a dedicated and persistent log server Monitor security events from VMs stored in system logs

III. PROPOSED SOLUTION

In the Presented Research Work, Consider Cloud-user, Cloud-verifiers, a Blacklisting controller and Cloud-provider are involved. Cloud-providers issue the membership certificate for the cloud-users. Blacklisting-controller can blacklist the membership certificate of the cloud user. The data can be accessed according to the need of the user as well as the cloud user can vary in the system. Let's take a situation where hardware enabled authentication-key in an ideally suited system. The process conceded through the authentication-key K are initialized, registered, membership approval and blacklisting. Let's take a circumstance where an equipment grounded validation key in a perfect framework. The methodology completed by the validation key K are introduced, enrolled, participation endorsement and blacklisting In this stage each component is dealt by the controller which is showed up by the approval-key. Clients are required to enlist. With K, client call for the authenticator and the authenticator queries the cloud-provider whether the customer can get enlisted. If the cloud-provider permits, the authenticator prompts the clients that individual can transform into a section. In the support affirmation mastermind, the authenticator will send a demand that authenticator needs to interact with the verifier. Using K, it requests the verifier that client needs to execute the enlistment affirmation devoid of disclosing to the verifier whom the authenticator is actually. Verifier picks a message s and sends s to the authenticator. In the event that the authenticator is not a part, K prematurely ends. Something else, K tells the authenticator whether he has been blacklisted and requests that he can continue. In the event that the authenticator is not prematurely ended, K gives the verifier a chance to perceive that a blacklisted buyers has marked the messages. Something else, K hint the verifier that s has been marked by a genuine part. Blacklist again send the solicitation for the enrollment confirmation. The blacklisting-controller says the authenticator to blacklist a client. On the off chance that the buyer is not a team part, K rejects the solicitation. Something else, K denote the customers as refused. A consumer who is not a part or is a part or refused by the controller can't be effective in participation acknowledgment to any verifiers. The verifier can't perceive in the enrollment endorsement who is the authenticator, along these lines indicating obscurity. Blacklist causes verifiers to dispose of messages marked by a blacklisted client in a perfect framework. In this tradition, if a purchaser's private-key is uncovered as well as the cloud customers is blacklisted, the signs from this blacklisted cloud buyers get the chance to be linkable to a true blue verifier. Thus, defiled buyers who uncover their private-keys and are blacklisted purposefully relinquish their security. In like manner, an authenticator could examine regardless of whether the customer have been blacklisted from on the-blacklist, earlier to the customer signs a stamp and delivers it to the verifier. If the authenticator discovers that the client has been blacklisted, he or she can decide on not to progress. The protection of proposed work relies on upon individuals in general key cryptographic convention and the Diffie-Hellman suspicion. The establishment of the general population key cryptographic as takes after.

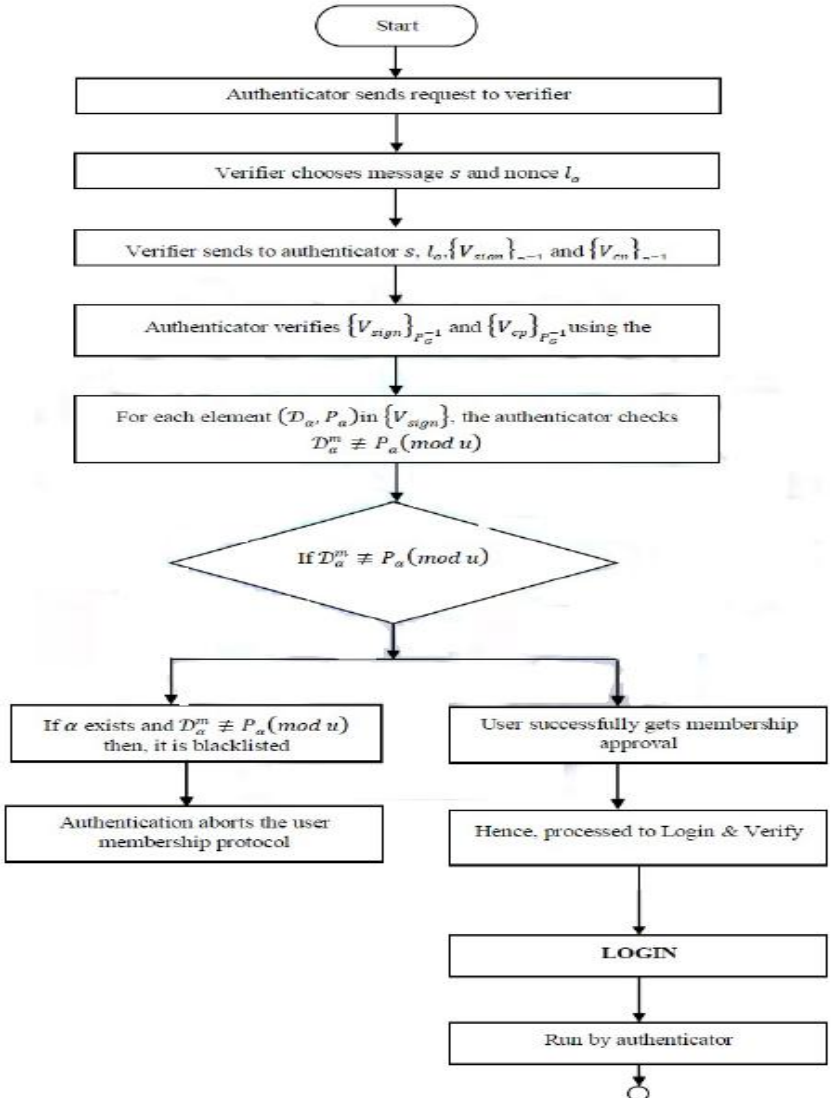

Figure 1: Registration Phase

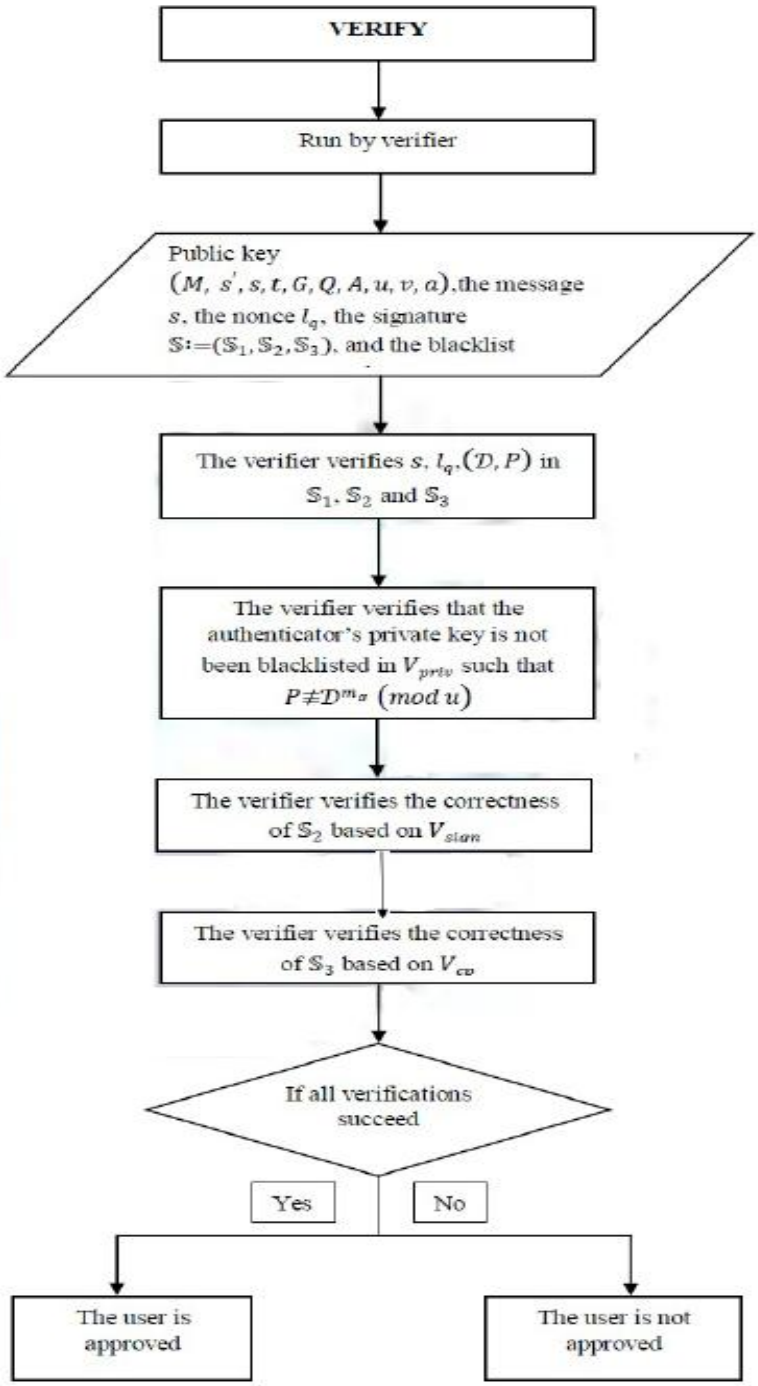

Figure 2: Verify Phase

IV. Evaluation of Result for SaaS CLOUD INFRASTRCTURE USING PORTABLE TPM

Presented system model specially designed on Visual-Studio 2012 platform 4.0 with programming language C sharp. Here Microsoft Azure platform is used for developing the overall system architecture. Here proposed thesis main goal is to prevent the data leakage which is an issue found typically in cloud-computing environment. Portable-TPM based end user authentication model is able to support key operations by making use of TPM devices in order to deliver much improved security and safety. Hence device portability is

accomplished. An end user can gain access to cloud services such as storage's details in safe environment and securely store user data to the remote cloud server making use of these particular portable devices which one offers additional protection.

Various user scenarios is considered for simulation 10, 20, 30, 40 and 50 and for all User attestation overhead is observed, memory utilization is observed and CPU performance is evaluated.

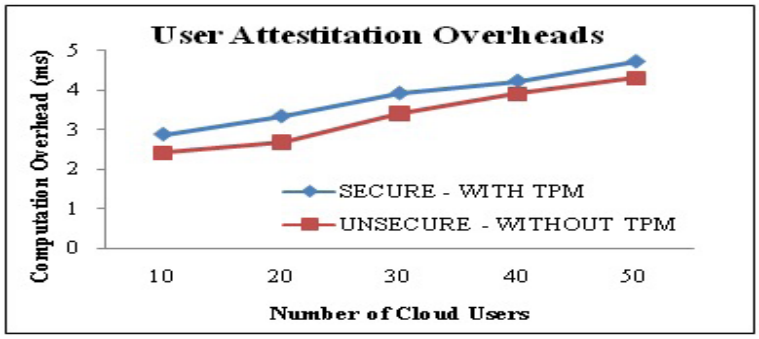

Figure 3: User Attestation Computation Overheads

Computation overhead for considering all five scenario user/ password. False user condition has less computation overhead due to in first attempt user is verified and once user is false further computation is stopped. While for correct user/password with false dongle computation is done for all user it matched then for password it also matched then for verification of all dongle which create more computation overhead. Here average computation overhead is taken for all five scenario for various user group such as 10, 20, 30, 40 and 50.

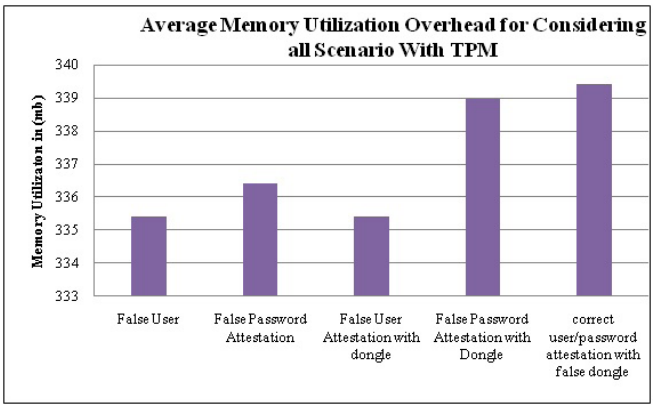

Figure 4: Average Memory Utilization Overhead for Considering all Scenario with TPM

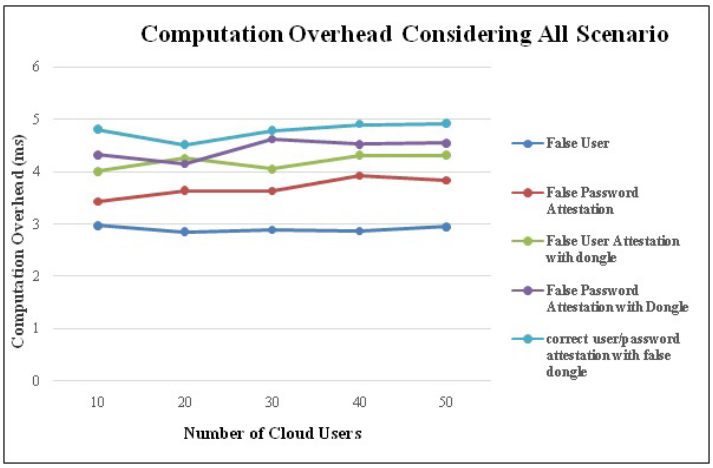

Figure 5: Computation Overhead Considering All Scenarios

Table 2: Average Computation Overhead

Computation Overhead Condition	Average Computation Overhead in (ms)
False User	3.88
False Password	3.91
False User with Dongle	3.99
False Password with Dongle	4.11
Correct User Password with False Dongle	4.12

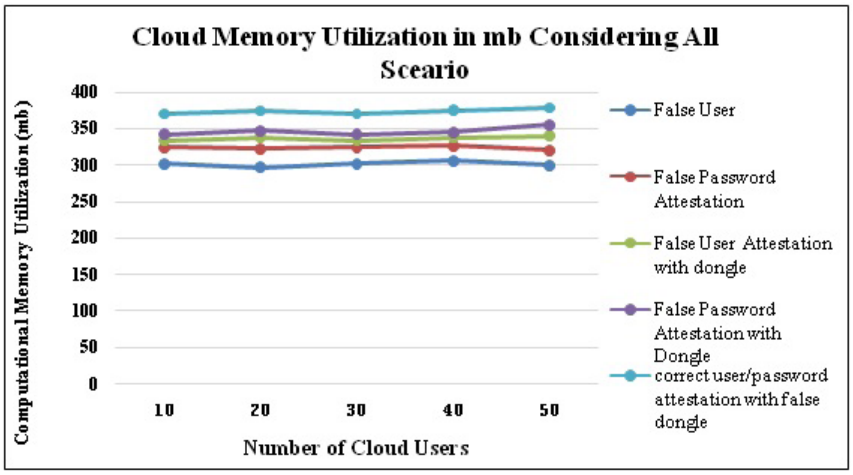

Figure 6: Cloud Memory Utilization in MB Considering All Scenarios

Cloud memory utilization is presented for all user group, utilized memory is presented here in megabyte. False user condition utilized less memory while correct user/password utilized more memory. Average cloud memory utilization is below Table considering all scenarios.

Table [3] : Average Cloud Memory Utilization

Cloud Memory Utilization Condition	Average Cloud Memory Utilization (MB)
False User	335.39
False Password	336.40
False User with Dongle	335.3973
False Password with Dongle	338.9679747
Correct User Password with False Dongle	339.4162338

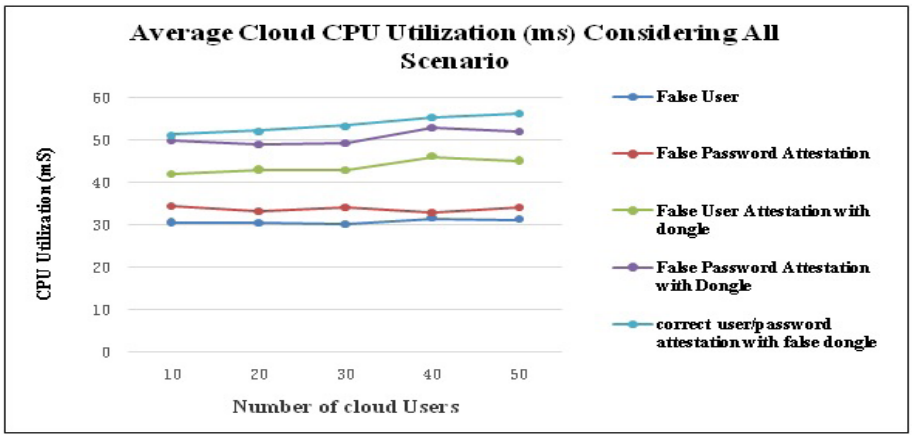

Figure 7: Average Cloud CPU Utilization (ms) Considering All Scenarios

Average cloud CPU utilization is presented for various user groups in figure above; here we are considering group size as 10, 20, 30, 40 and 50. CPU utilization is presented is presented for all with TPM. Overall average memory utilization with TPM device for all different scenarios is given in table

Table 2 : Average Cloud Memory Utilization

Cloud Memory Utilization Condition	Average Cloud Memory Utilization (ms)
False User	41.58
False Password	41.51
False User with Dongle	41.89
False Password with Dongle	43.68
Correct User Password with False Dongle	43.71

V. CONCLUSION

The subsequent advantages of using the TPM hardware are it is less computational effort for trusted-hardware-device, portability and additional highly effective blacklist mechanism. The primary design process is that the host as well as the hardware collectively performs the membership-approval as the authenticator. The cloud offers services/ resources on demand and the cost of provisioning services by cloud provider is based on pay-per-usage of cloud instances/virtual machine. The adoption of cloud technology for deployment of organization computation usage involves certain security risk associated with it such as remote user attestation and secure SaaS attestation and so on. Earlier used security system is not able to resolved the security issues pertaining in the cloud system. At the time of cloud infrastructure deployment security issues must be addressed and resolved effectively and cost of secure cloud is also must be considered. Security is an important parameters which must be considered in cloud computing for secure and safe computation in the cloud. For that a secure authentication process is needed to verify the cloud model over the internet such as SaaS on public cloud environment

REFERENCES

[1]. J Winter, Trusted computing building blocks for embedded linux-based ARM trust zone platforms, 3rd ACM workshop on Scalable trusted computing., (2008), 21-30.

[2]. Najwa Aaraj and Niraj K Jha, Analysis and design of a hardware/software trusted platform module for embedded systems, ACM Transactions on Embedded Computing Systems., 8 (2008),

[3]. Jorge Rodrigues, , Software as a Service Value and Firm Performance-A literature Review Synthesis in Small and Medium Enterprises, Nanjing., 16 (2014), 206-211.

[4]. D. Thilakanathan, R. Calvo, S. Chen and S. Nepal, Secure and Controlled Sharing of Data in Distributed Computing, IEEE 16th International Conference on Computational Science and Engineering., (2013), 825-832.

[5]. .S. Han and J. Xing, Ensuring data storage security through a novel third party auditor scheme in cloud computing, IEEE International Conference on Cloud Computing and Intelligence Systems., (2011), 264-268.

[6]. C. Senk and F. Dotzler, Biometric authentication as a service for enterprise identity management deployment: a data protection perspective, Sixth International Conference on Availability, Reliability and Security., (2011), 43-50.

[7]. J. Du, D. J. Dean, Y. Tan, X. Gu and T. Yu, Scalable Distributed Service Integrity Attestation for Software-as-a-Service Clouds, IEEE Transactions on Parallel and Distributed Systems., 25 (2014), 730-739.
[8]. Shyam Nandan Kumar, Amit Vajpayee ,A Survey on Secure Cloud: Security and Privacy in Cloud Computing, American Journal of Systems and Software ,Vol. 4, No. 1(2016) 14-26.
[9]. Saxena S, Sanyal G and Srivastava S, Mutual authentication protocol using identity based shared secret key in cloud environments, Recent Advances and Innovations in Engineering., (2014), 1-6.
[10]. Juan Du, Dean, D.J, Yongmin Tan, XiaohuiGu and Ting Yu, Scalable Distributed Service Integrity Attestation for Software-as a Service Clouds, IEEE Transactions on Parallel and Distributed., 25 (2014), 730-739.
[11]. M. Burnside and A.D. Keromytis, End-to-End Protection of Sensitive Information in Web Services, 12th International Conference Information Security., (2009), 491-506

Dr. Pramod" Securing SaaS Cloud Infrastructure Using Portable TPM." International Journal of Computational Engineering Research (IJCER), vol. 08, no. 08, 2018, pp. 67-75.