DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4700

ISSN No. 0976-5697

Volume 8, No. 8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

PRIVACY ENHANCEMENT IN CLOUD ENVIRONMENT THROUGH TRUSTED THIRD PARTY APPROACH

Getasew Nibretu Yirdew
Department of Computer Science and Systems Engineering
College of Engineering (A), Andhra University
Visakhapatnam, India

Sheik Khadar Ahmad Mnoj
Department of Computer Science and Systems Engineering
College of Engineering (A), Andhra University
Visakhapatnam, India

Prof.D. Lalitha Bhaskari
Department of Computer Science and Systems Engineering
College of Engineering (A), Andhra University
Visakhapatnam, India

Abstract: Cloud computing is an established approach in the current IT industry which provides web-based services, computations, and storage facilities to the end-users including business, healthcare, and government institutions. It offers dynamically scalable resources, on-demand services through which the customers are economically benefited by availing any of the resources and services. In the traditional way of cloud computing there is a possibility for the cloud service providers (CSP) to view, access, modify, and monitor the utilized resources of the cloud customers thus the privacy is a major concerns for a cloud customers (CC), especially when sensitive data such as personal profile, financial records, medical reports, etc. are outsourced to the cloud server. In this paper, a model is proposed to support primarily the privacy issues of the customers and providers by incorporating the concept of the trusted third party (TTP) that can manage the computing process held on between CC and CSP without revealing their identities to each other. The trusted third party is an autonomous system that facilitates secured communication between the two parties and it ensures a customer to have high-level of trust on cloud providers by guarantying the privacy protection of the data.

Keywords: Cloud Computing Services; Data Security and Integrity; Trusted Third Party; User Authentication; privacy; Trust

I. INTRODUCTION

Cloud computing is a new approach in the IT industry that can be used as a platform for delivering a convenient and on-demand network-based access from a shared collection of configurable computing resources like networks, storages, servers, applications, and services based on a pay per usages basis through the internet. Resources and services on the cloud can be rapidly provisioned and released with a minimum of management effort or a little service providers' interaction. Nowadays the cloud computing model can be categorized into five key characteristics, three delivery models, and four deployment models. The five major characteristics of the cloud computing models are:

- On-Demand Self-Service
- Ubiquitous Network Access
- Location Independent Resource Pooling
- Rapid Elasticity and
- Measured Service

The above-listed characteristics of a cloud computing models are in common all of these geared towards using clouds seamlessly and transparently. In general, Cloud computing provides:

1. *Resources are on-demand*: That means when the customers want the service immediately they can able to access it and this is made possible by self-service and automation. Self-service means that the consumer performs all the actions needed to acquire the service themselves. The consumer's request is then automatically
2. processed by the cloud infrastructure, without human intervention on the provider's side.
3. *Rapid Elasticity:* The elasticity approach of a cloud computing model is used for the cloud customers to perform a quickly scale up or down resources and services.
4. *Measured Services:*
   These are primarily derived from business model properties and indicate that cloud service providers control and optimize the use of computing resources through automated resource allocation, load balancing, and metering tools. Despite this, applications running (deployed) on or being developed for cloud computing platforms are affected by various security and privacy challenges depending on the basic delivery and deployment models.
5. *Ubiquitous network access:* This enables clients to access and use the services from the cloud everywhere and at any time.
6. *On the other hand location*, independent resource pooling is main characteristics of cloud computing where resources and services are available and easily accessible on the internet.

The second categories of cloud computing models are that the three key cloud delivery models, which are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In the IaaS, the cloud provider supplies a set of virtualized infrastructural components as a service, like virtual machines (VMs), abstracted hardware, operating systems(OS), and storages on which customers can access resources and use services and

developers also can build and run applications through a service called Application Programming Interface(API). The application will eventually reside on the VM and the virtual operating system. On the other hand, there are some critical issues such as trusting the VM image, hardening hosts, and securing inter-host communication are critical areas in IaaS. The second cloud delivery models are PaaS that allows programming environments to access and utilize additional application building blocks. These programming environments have a visible impact on the application architecture, such as constraints on which services the application can request from an OS. For example, a PaaS environment might limit access to well-defined parts of the file system, thus requiring a fine-grained authorization service. The figure below shows the three key cloud delivery models relationship with examples:

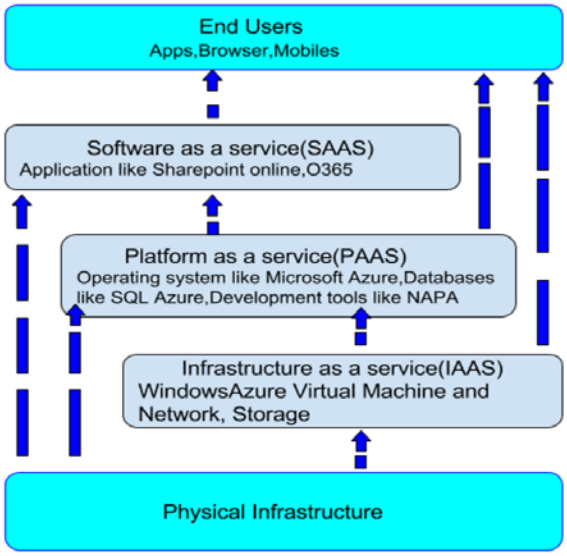

Fig. 1: Cloud Service Models [2].

In general, the delivery of a solution stack for software development includes a runtime environment and lifecycle management software. This allows customers to develop a new application using APIs deployed and configurable remotely. Examples include Google APP Engine, forece.com, and Microsoft Azure. Finally, in SaaS models, the cloud providers enable and provide application software as on-demand services. Because clients acquire and use software components from different providers, crucial issues include securely composing them and ensuring that information handled by these composed services is well protected. Example are included online word processing and spreadsheet tools, customer relationship management (CRM) services and web content delivery services (like Salesforce CRM, Google Docs, etc.).

To protect the issues of losing sensitive data from unauthorized access, different methods can be used. Generally, before storing data in the cloud, it is encrypted using various algorithms [1]. Though the toughest encrypted techniques also do not guarantee fully as hackers and unauthorized people can compromise its integrity.

Cloud computing has several deployment models includes public, private, community and hybrid clouds. Public clouds are external or publicly available on cloud environments that are accessible to multiple tenants, whereas private clouds are typically personalized environments with dedicated virtualized resources for particular individuals or organizations. Similarly, community clouds are targeted for particular groups of customers or groups of small business groups. Hybrid clouds are another cloud deployment model that is a combination of public and private, public and community or private and community [2].

Roles in Cloud Computing can be defined as the responsibilities, access, and profile of different users that are part of a cloud computing solution. The following figure presents these roles defined in the three service layers [7]. The provider is responsible for managing, monitoring and guaranteeing the availability of the entire structure of the cloud computing solution. It frees the developer and the final user from such responsibilities while providing services in the three layers of the architecture. Developers use the resources provided by IaaS and PaaS to provide software services for final users. This multi-role organization helps to define the actors (people who play the roles) in cloud computing environments. Such actors may play several roles at the same time according to need or interest. Only the provider supports all the service layers.

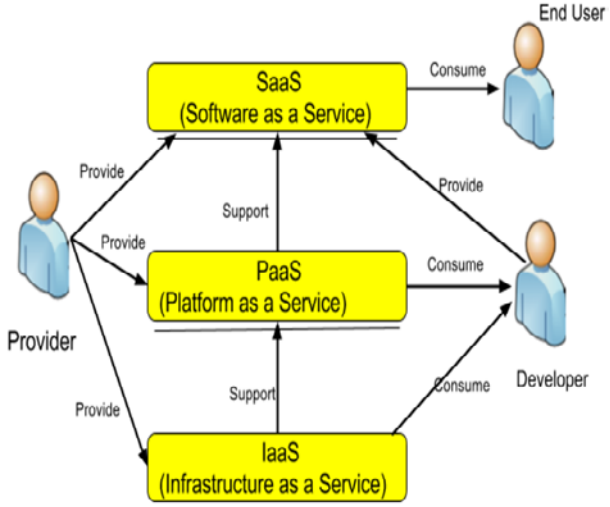

Fig. 2: Roles in Cloud Computing [4].

Cloud computing services have suffered security and privacy issues at a high level. Clearly, many privacy and security attacks occur from within the Cloud provider themselves as they usually have direct access to stored data and steal the data to sell to third parties in order to gain profit. In this paper, a model is called trusted third-party proposed to overcome the above problems by hiding the customer's identity from the cloud provider. The TTP is a security and privacy-enhancing approach which acts as a delivery channel between customers and service providers.

II. LITERATURE REVIEW

The main advantages of implementing a Trusted Third Party approach in the cloud environment is to the establishment and assurance of the necessary Trust level and provides ideal solutions to preserve the security, confidentiality, Privacy, integrity, and authenticity of data and communications[3]. In the traditional way of cloud computing, a customer has to trust the providers without any other choices. Therefore the TTP approach removes a necessary trust or dependent of customers only on their providers instead they will have a chance trust the third party and they have a benefit to hide their details from their providers. Accordingly, this, a trusted third party (TTP) is an entity or middleware server which facilitates a secure communication or interactions between two parties providers and customers who both trusts this third party. In addition to this, a TTP in a cloud system is used to provide end-to-end secure communication services, which are scalable, based on

standards and importance across different domains, geographical areas, and specialization sectors. The establishment and the assurance of a trusted relationship between two mutually communicating parties i.e. customers and providers should be concluded as a result of specific acceptances, techniques, and mechanisms.

The major roles of TTP server that it reviews all critical transaction communications between the parties, based on the ease of creating fraudulent digital content. The Introduction of a trusted third party can partially address the problem of loss of the traditional security and privacy boundary by creating trusted security domains. As described by Castell, ‘‘A Trusted Third Party is an impartial organization delivering business confidence, through commercial and technical security features, to an electronic transaction. Accordingly Castell, the TTP provisions technically and legally reliable as well as trusted means of carrying out, facilitating, producing independent evidence about and/or arbitrating on an electronic communication transaction. Its services are provided and underwritten by technical, legal, financial and/or structural means’’ [4]. This infrastructure leverages a system of digital certificate distribution and a mechanism for associating these certificates with the known origin and target sites at each participating server.

TTP services are provided and underwritten not only by technical, but also by legal, financial, and structural means [4, 5]. TTP are operationally connected through chains of trust (usually called certificate paths) in order to provide a web of trust forming the notion of a Public Key Infrastructure (PKI). Public Key Infrastructure provides technically sound and legally acceptable means to implement [6]:

Atallah et al. [8] [9] gave two protocols later that were used for secure sequence outsourcing and algebraic computation outsourcing. Since these two protocols used burdened cryptography algorithm like homomorphic encryption [10]. Thus were not very successful for large problem set due to huge complexity.

Based on above concept, Hohenberger [13] defined secure outsourcing protocols of modular exponentiation, which was taken to be a public key cryptography method that was very expensive. Latest, Atallah [13] et presented safe protocols based on secret key concepts for secure outsourcing that used matrix multiplication [14]. This assumption performed very well due to the assumption of only one server and computation effectiveness. The only lacking point is a lot of overhead because of message passing. Concluding, these methods are still not efficient enough for secure IP outsourcing computation.

1. *Strong Authentication:*
The control of authenticity, the process of identification of parts involved in electronic transactions or exchange of information with electronic means.

2. *Authorization:*
The authenticated access to resources, database, and informative systems, according to the user’s permission rights and the roles.

3. *Data Confidentiality:*
The protection of information either locally or remotely store d or in transmission from unauthorized access.

4. *Data Integrity:*
The protection of information either locally or remotely stored or in transmission from unauthorized deletion, readi ng or modification.

5. *Data Availability:*
Storage service providers (SSPs) to describe products and services that ensure that data continues to be available at a required level of performance in situations ranging from normal through "disastrous."

6. *Data Privacy:*
Enable users to have control over their data when the data are stored and processed in cloud and avoid theft, nefarious use, and unauthorized resale.

The trusted third party can rely upon Low and High-level confidentiality, Server and Client Authentication, Creation of Security Domains, Cryptographic Separation of Data, Certificate-Based Authorization.

Cloud computing has main characteristics like the ability to grow up rapidly, store big data remotely, and deliver shared resource and services in a dynamic environment. As technology advances, organizations are increasingly turning to cloud-based solutions to solve the challenges posed by the increasing costs of traditional infrastructure. However, cloud-based solutions cause some challenges, mainly where personal data is being stored, how personal data is being retrieved from the cloud as well as what is really going on the cloud. The following are some of the critical issues of cloud computing [7]

1. *Security and Privacy Issues:*
Security is a fundamental issue (challenges) for users in cloud computing. I.e. users are not sure that how much their data are safe whereas Privacy entails the protection and full control of the personal information of customers, and the meeting of expectations of customers about its use but in cloud data are out of clients monitoring.

2. *Possible Downtime:*
Cloud computing is fully Internet-based services, that means when there is no internet connectivity service will be stopped. So your business depends on how much your (users) internet speed is enough good and for how long time it will be available. Unless it will not be suitable services.

3. *Cloud Providers Reliability:*
Cloud computing service providers suffer server outages (service unavailability) frequently.

4. *Inflexibility:*
The inflexibility of some cloud applications can be another serious disadvantage of cloud computing. It needs a clear understanding when choosing a cloud computing vendor that you're not going to become a "forever" customer because their applications and/or data formats may not allow easily transfer/conversion of information into other systems.

5. *Customer Support:*
If your business needs are such that you need a rapid response to customer care issues, make sure that your cloud services vendor has plenty of options available for technical support, including email, phone, live chat, knowledge bases, and user forums.

III. PROPOSED METHODOLOGY

Traditional security approach still requires users to trust their cloud service providers (CSP). However, the trusted third party (TTP) approach removes the need for the user to trust their service provider. The proposed system is used to enhance the security and privacy issues of cloud user's data through a trusted third party and it overcomes the need of users to trust their provider. The TTP is fully trusted by customers and providers which assist the communication among the two parties (client and provider) who both trust this third party, and the third party examines all critical data

flows between the parties to perform accordingly their interest. In TTP the security issue of cloud can be addressed by hiding the customer's identity details from the providers, i.e. providers can't know whose data is stored on their storage server. The TTP tries to dynamically assign the customers who required services and resources with the providers who offered services and resources on the cloud-based on the requirement that fits their need. The proposed system has four main functionalities which are depicted in figures below.

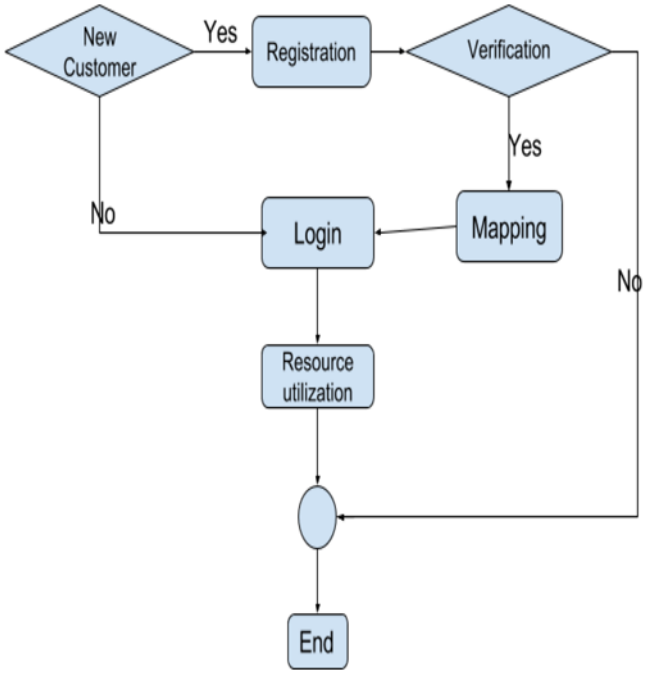

Fig. 3: Overview of the Proposed Methodology

1. ***Registration and Verification****:*

In the registration process, details of cloud users and providers are recorded in the database and they will get username and password for login to the cloud. Customers have to agree on the payment per the services they will use. Once if the customer is agreed upon the payment they will wait for some time until approval is done. Both user's and provider's status will be checked and authentication process will be done. In the approval process, the trusted third party (server) will verify the details provided by them, if TTP is satisfied he will approve their registration by sending an email with the credentials otherwise will be rejected The following table shows sample data format for registered customers.

Table 1: Customer and Providers Registration

ID	Full Name	User Name	Email	address	City	Phone Number	Services Required	Remark

The figure below depicts a trusted third party model that shows the registration process for the two-party and among this those customers and providers which are not failed authentication process are indicated by "rejected" and those who approval processes are correct are marked as "approved".

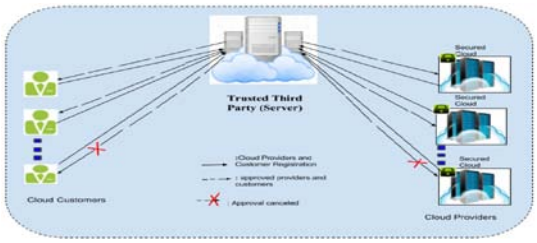

Fig. 4: Registration and Verification process on the TTP.

2. ***Login:***

Authorization is a technique to gain access to the system services. a cloud provider will provide services and the customer will get the services and resources. Once login process is successful then customers can start accessing the services by logging at the TTP server.

3. ***Mapping Process:***

The TTP will assign each authenticated cloud customer to a verified cloud provider. The TTP will use a dynamic algorithm for this mapping process. The interesting factor here is that neither the provider nor the customer knows to whom they have been assigned. After customer/provider gets an assignment or mapping a notification email will be delivered to them to inform them as they can start the services. The CC starts using the service without the knowledge of to which provider they have been assigned to and the same is the case with the provider, they offer the service without really knowing to which customer they are offering the service.

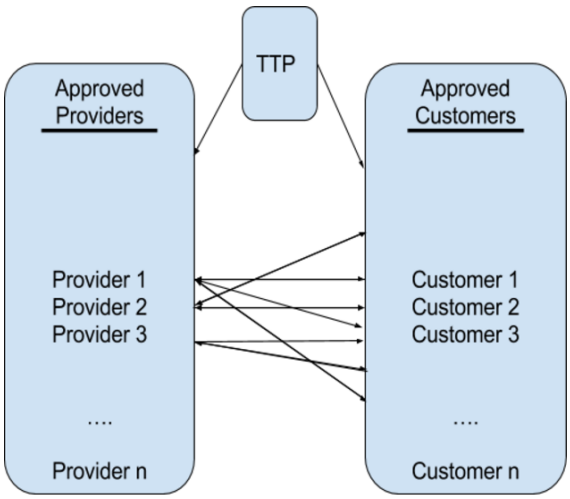

Fig 5: a process for resource allocations.

4. ***Service Usage:***

Cloud Customers after the resource usage, they will receive the bills from TTP. The TTP after receiving the payment from the Customer will deduce some amount and pay the remaining to the provider. In this proposed system, the service usage without the intervention of TTP is not possible which will help the remaining users to have trust in the process.

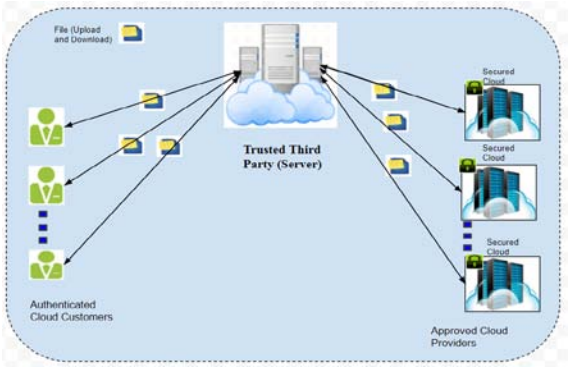

Fig. 6: Trusted Third Party Architecture for Cloud Service.

The proposed system model has three components:

1. Cloud Customers
2. Cloud Provider
3. Trusted third party

1. *Cloud Customers:*

A client or end users which need cloud services. In this proposed system each customer is used cloud services models. The inclusion of new user is made by registering and providing a new customer id by the TTP. The following table shows the customers and providers relationship.

2. *Cloud Providers:*

Providers are companies who aim is to deliver different kinds of cloud services models. These people details will be registered at the TTP server and they will get the payment for the services provided by them. The CSP will provide all necessary documents and gets approval from the TTP to be part of the proposed system. Once after they start to deliver services and resources they can check and know how many customers are getting their service and the total income they earn.

3. *Trusted third party:*

Certified agencies (servers) who can serve as a middleware (server) among clients and providers. This agent performs approval and authorization for both users and providers as well as monitoring all activities performed by them. If he finds anyone is ambiguous he will delete his account and charge him for the damage caused by him. Generally, below is the flowchart of the proposed system model that depicts all the activity done by the user and provider.

IV. CONCLUSION

In recent years, cloud computing has gained importance, especially in resource and service sharing. The widespread dissemination of smartphones and portable devices and a better way of designing secured infrastructure are the main factors in driving the growth and acceptance of cloud computing. On the other hand, Cybercriminal activities are impacting cloud computing environments with multiple, and potentially conflicting challenges related to security and privacy which are major threats that can undermine customer's confidence in the cloud. In this paper, a secured framework has been proposed which utilizes the concept of the trusted third party to address the security and privacy issues which are being threats for cloud customers. The proposed framework emphasizes on authentication of clients and providers without revealing their identities to each other. The major advantage here is, this model shields data from targeted attacks as the parties' identities are not disclosed. This models main drawback is it is a single point failure, where if the trusted third-party is compromised then the total concept of privacy will be violated. Therefore it is recommended that protection should be given merely only on the TTP servers which will benefit the CC and CSP parallel.

V. REFERENCES

[1] M.J.Atallah, K.N.Pantazopoulos, J.R. Rice, and E.H. Spafford, "Secure Outsourcing of scientific

[2] computations", Adv. Comput., vol.54, pp. 216-272, 2001.

[3] Mell, P., & Grance, T. (2009). NIST Definition of Cloud Computing. Retrieved from

[4] NIST www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

[5] D. Polemi, Trusted third-party services for healthcare in Europe, Future Generation Computer Systems 14 (1998) 51–59.

[6] S. Castell, Code of practice and management guidelines for trusted third-party services, INFOSEC Project Report S2101/02, 1993.

[7] Commission of the European Community. Green paper on the security of information systems, ver. 4.2.1, 1994.

[8] VeriSign. Directories and public-key infrastructure (PKI), Directories and Public—Key Infrastructure, PKI.

[9] http://www.cloudsecurityalliance.org/ Top Threats Working Group the Notorious Nine Cloud Computing Top Threats in 2013.

[10] A. Marinos and G. Briscoe, "Community cloud computing," in First International Conference Cloud Computing, CloudCom, volume 5931 of Lecture Notes in Computer Science, pp. 472–484. Springer (2009).

[11] S. Hohenberger and A.Lysyanskaya, "How to securely outsource cryptographic computation", in Proc. 2nd Int.Conf. Theory Cryptography, 2005, pp. 264-282.

[12] M.J.AtallahandJ.Li.,"Secure outsourcing of sequence comparisons," in Int. I. Inf. Sec., vol. 4, no. 4, pp. 277-287,2005.

[13] D.BenjaminandM.J.Atallah,'Privateandcheating-free outsourcing of algebraic computation," in Proc. Int. Conf. Privacy, Secur., Trust, 2008, pp. 240-245.

[14] M. Atallah and K. Frikken, "Securely outsourcing linear algebra computations," in Proc. of ASIACCS, 2010, pp. 48–59.

[15] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. 17th Int. Conf. Theory Appl. Cryptographic Tech., 1999, pp. 223–238.

[16] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.