ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS VOLUME 1, ISSUE 4, OCTOBER 2014, PP 240-244

Well-Organized Security Solution for Privacy Preserving Cloud Services

M.Asma Farheen [1], M.Manasa [2], B.Ragalatha [3],Ms. K.Lakshmi [4]
Department of IT, G.Pullaiah College of Engineering and Technology. Kurnool
JNTU Anatapur, Andhra Pradesh, India

Abstract:- The cloud computing could be a new computing model that comes from grid computing, distributed computing, parallel computing, virtualization technology, utility computing and alternative laptop technologies during this paper, we have a tendency to present a unique privacy-preserving security resolution for cloud services. We have a tendency to wear down user identification and secure communication. Our resolution provides solely registered users to access cloud services. Our resolution offers anonymous authentication. This implies that users' personal attributes (age, valid registration, and successful payment) may be proved while not revealing users' identity. Our resolution offers secure communication of transmitted information.

Key Terms: Cloud Service Provider, RSA public key, privacy-enhancing technologies (PET's), standards development organizations (SDOs)

I. INTRODUCTION

The cloud computing becomes the host issue in trade and world with the fast development of constituent and software package. The cloud computing is that the results of several factors like ancient technology and communication technology and business mode. It supported the network and has the format of service for the buyer. The cloud computer system provides the service for the user and has the character of high measurability and dependableness. The resource within the cloud system is clear for the appliance and also the user don't grasp the place of the resource. The users will access your applications and information from anyplace. Resources in cloud systems are often shared among an oversized range of users. The cloud system might improve its capability through adding additional hardware to affect the increased load effectively once the work load is growing. Cloud resources are provided as a service on Associate in nursing pro re natal basis. The cloud itself generally includes giant numbers of commodity-grade servers, controlled to deliver extremely scalable and reliable on-demand services. The number of resources provided within the cloud system for the users is increased after they want additional and reduce after they want less. The resources are often the computing, storage and different specification service. The cloud computing is seen because the vital modification of knowledge trade and can build additional impact on the event of knowledge technology for the society. There are few science tools that may each hide user identity and supply secure communication. The suppliers of cloud services ought to management the authentication method to allow the access of solely valid purchasers to their services. In follow, many users will access cloud services at a similar time. Hence, the verification method of user access should be as economical as potential and also the process science overhead should be least. We have a tendency to propose a unique security answer for cloud services that provides anonymous authentication. We have a tendency to aim principally on the potency of the authentication method and user privacy. Our answer conjointly provides the secure communication and privacy of transmitted information between users and cloud service suppliers.

II. RELATED WORK

Just some year's agone, folks won't to carry their documents around on disks. Then, additional recently, many folks switched to memory sticks. Cloud computing refers to the power to access and manipulate info hold on remote servers, victimization any Internet-enabled platform, as well as Smartphone's. Computing facilities and applications can progressively be delivered as a service, over the net. we have a tendency to are already creating use of cloud computing once, for instance, we have a tendency to use applications like Google Mail, Microsoft Office365 or Google Docs. Within the future, governments, firms and people can progressively address the cloud. The cloud computing paradigm changes the approach during which info is managed, particularly wherever personal processing worries. End-users will access cloud services while not the requirement for any skilled information of the underlying technology. this can be a key characteristic of cloud computing, that offers the advantage of f reducing value through the sharing of computing and storage resources Privacy, during this report, refers to the correct to self-determination, that is, the correct of people to 'know what's celebrated regarding them', remember of hold on info regarding them, management however that info is communicated and stop its abuse. In different words, it refers to quite simply confidentiality of knowledge. Protection of private info (or information protection) derives from the correct to privacy via the associated right to self-determination. each individual has the correct to manage his or her own information, whether or not personal, public or skilled while not information of the physical location of the server or of however the process of private information is configured; end-users consume cloud services with none info regarding the processes concerned. Information within the cloud are easier to govern, however conjointly easier to lose management of. As an example, storing personal information on a server somewhere in computer network might create a significant threat to individual privacy. Cloud computing therefore raises variety of privacy and security queries. Will cloud suppliers be trusted? Are cloud servers reliable enough? What happens if information gets lost? What regarding privacy and lock-in? Can shift to a different cloud be difficult? Privacy problems are progressively vital within the on-line world. It's typically accepted that due thought of privacy problems promotes user confidence and economic development. However, the secure unleash, management and management of private info into the cloud represent an enormous challenge for all stakeholders, involving pressures each legal and business. This report analyses the challenges posed by cloud computing and also the standardization work being done by varied standards development organizations (SDOs) to mitigate privacy risks within the cloud, as well as the role of privacy-enhancing technologies (PETs)

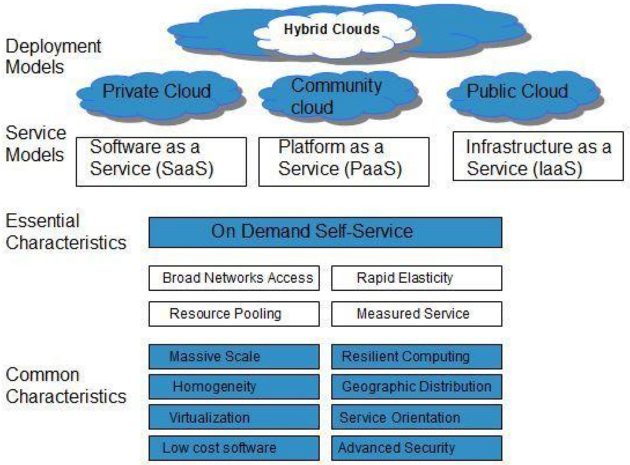

Fig 1 .Over view of Cloud Computing

CLOUD COMPUTING PARADIGM AND PRIVACY

The cloud model promotes availableness and consists of 5 essential characteristics, 3 delivery models and 4 preparation models. The 5 key characteristics of cloud computing square measure on-demand self service, present network access, location-independent resource pooling, speedy snap and measured service, all of that square measure geared towards seamless and clear cloud use. Speedy snap permits the scaling up (or down) of resources. Measured services square measure primarily derived from business model properties whereby cloud service supplier's management and optimize the utilization of computing resources through automatic resource allocation, load equalization and metering tools.

The 3 cloud service delivery models (see figure 1) are: Application/Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). ITU Technology Watch revealed a separate report on the cloud computing development in March 2009 [15]. These 3 classic cloud services models have totally different divisions of responsibility with relevance personal information protection. The risks and edges related to every model also will take issue, and want to be determined on a item-by-item basis in reference to the character of the cloud services in question SaaS permits the buyer to use the provider's applications running on a cloud infrastructure. The applications square measure accessible from varied consumer devices through a consumer interface like an internet browser (e.g. web-based email like Gmail or CRM from Salesforce). With the SaaS model, the buyer has very little or no influence however input file is processed however ought to be ready to think about within the cloud provider's responsibility and compliance or will management that input he provides to a SaaS. 1st of all he will avoid giving smart information to a SaaS. second he could be ready to "secure" the smart information before he inputs them into the SaaS (e.g. their exists plug-in for browsers supporting encoding of input from fields. this might be wont to send solely encrypted mails exploitation Gmail).

PaaS provides tools, supported by a cloud supplier, that modify developers to deploy applications (e.g.Salesforce's Force.com, Google App Engine, Mozilla Bespin, Zoho Creator). On the one hand, a giant responsibility lies with the developer to use best practices and privacy-friendly tools. On the opposite hand the developer should think about the trustiness of the underlying PaaS (and connected infrastructure). Assume as an example that some developer has developed a cloud application that encrypts all information before it's hold on among the cloud storage provided by the PaaS. During this case the developer should trust that the platform/infrastructure isn't compromised. Otherwise the assaulter may get access to the clear text (i.e. before encoding happens) – as a result of he wills management the execution atmosphere (e.g. virtual machine monitors hardware etc.).

IaaS provides the buyer with computing resources to run software system. One example of IaaS is Amazon EC2 internet Services. AN IaaS supplier can generally take responsibility for securing the information centers, network and systems, and can take steps to make sure that its workers and operational procedures suits applicable laws and rules

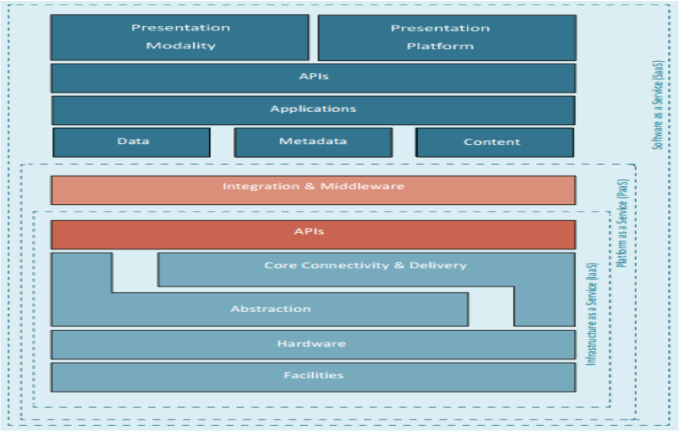

Fig 2. Cloud Security Alliance

III. OUR SOLUTION

In this we introduce our security solution for privacy preserving cloud services. We outline our system model, Security requirements, architecture and algorithm.

A. Model of our System

Our solution consists of two fundamental parties: •

Cloud Service Provider (CSP). CSP manages cloud services and shared storages. CSP is usually a company which behaves as a partly trusted party. CSP provides cloud services, authenticates users when they access a cloud service.CSP also issues access attributes to users. Nevertheless, when CSP needs to revoke and identify a malicious user hen CSP must collaborate with a revocation manager.

• User (U). U is an ordinary customer who accesses into a cloud and uses cloud services, shared storages, etc.Users are anonymous if they properly follow the rules of CSP. To increase security, users use tamper resistant devices or protected local storages.

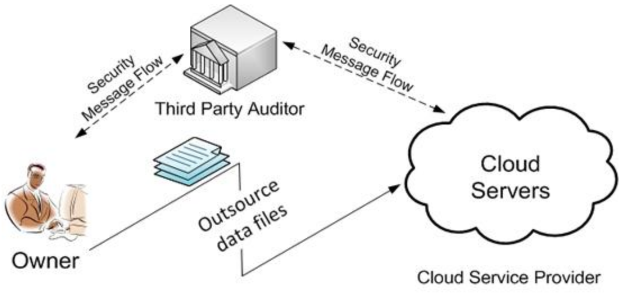

Fig 3. Architecture of Cloud Service Provider

B Necessity

Anonymity. Every honest user stays anonymous when uses cloud services. User identities are hidden if users behave honestly and do not break rules. Confidentiality. Every user's session to CSP is confidential. No one without a secret session key is able to obtain data transmitted between U and CSP.

C. Proposed Architecture

This proposed architecture is enhanced security model for cloud services like data storage. It consist of CSP i.e. loud Service Provider and user's.

Cloud Service Provider: - CSP generates a pair of keys i.e. secret key and public key by using cryptography algorithm RSA. CSP stores its own private key generated RSA algorithm and public key is shared by all.

User's:- User's must physically register on CSP. CSP check user's id. If user is already registered then there are some messages exchanged between users and CSP for establishing secure communication between them. User's generated a random request and encrypts this random request with the RSA public key of CSP and sends this request message to the server. Now server verifies this request if it is verified then server decrypt this message by using RSA secret key of CSP and generate a random key K_sym. Now with the help of this random key server generates a response by applying the X-OR operation to random and K_sym.Server send this response to user's. User's use this

Random key for file uploading and downloading and attain secure communication

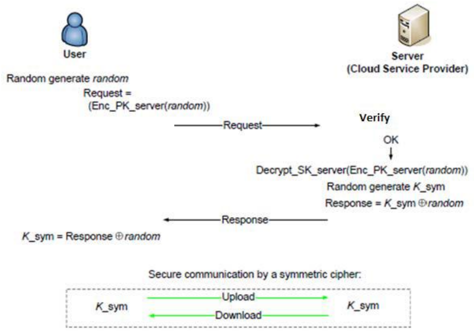

Fig 4: Architecture for proposed protocol

D. Proposed Algorithm

Key Generation: - The CSP generates the random key pair (Pk, Sk). Two large prime numbers P, Q are generated such that N=PQ (N is 1024 bits) and φ= (P-1)(Q-1) Select a random number 1<e<φ such that gcd (e,φ)=1. Compute the unique integer d=e-1(mod φ (n)).Where Pk (e, N) is the Public Key and Sk (d, N) is the Secret Key.

Secure Communication: - RSA provides the secure communication between client and server. Users encrypts random by the RSA public key of CSP. The encrypted Enc PK server (random) is send to the server. Server verifies the encrypted Enc PK server (random) if it verify then the server decrypt this with its secret key and generate random key K_sym.Compute the Response = K_sym random. CSP sends a response message (random K sym) back to user.

File Upload and Download:-The user can upload and download data to CSP. Data privacy is secured by a Symmetric cipher. We propose to use AES which is well known cipher and is supported by many types of software and hardware platforms. To encrypt and decrypt transmitted data, User and CSP use the AES secret key K sym established in the previous phase.

IV. CONCLUSSIONS

This paper presents resolution that offers user obscurity in authentication section and confidentiality throughout file Uploading and downloading for all users. Our authentication section is additional economical than connected solutions on the consumer aspect and conjointly on the server aspect because of missing valuable additive pairing operations and fewer involution operations. Because of this reality, cloud service suppliers victimization our resolution will manifest additional purchasers within the same time. We have a tendency to handle user anonymous access to cloud services and shared storage servers. Our resolution provides registered users with anonymous access to cloud services.

REFERENCES

[1] Y. Chen and R. Sion, "On securing untrusted clouds with cryptography," in Proceedings of the 9th annual ACM workshop on Privacy in the electronic society. ACM, 2010, pp. 109–114.

[2] R. Laurikainen, "Secure and anonymous communication in the cloud," Aalto University School of Science and Technology, Department of Computer Science and Engineering, Tech. Rep. TKK-CSE-B10, 2010.

[3] Sushmita Ruj, Milos Stojmenovic and Amiya Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds"in proceedings of the 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing

[4] Debajyoti Mukhopadhyay, Gitesh Sonawane, Parth Sarthi Gupta,Sagar Bhavsar, Vibha Mittal." Enhanced Security for Cloud Storage using File Encryption" Department of Information Technology Maharashtra Institute of Technology

[5] Kawser Wazed Nafi1,2, Tonny Shekha Kar2, Sayed Anisul Hoque3,Dr. M. M. A Hashem4, " A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture"in proceeding of the (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2011

[6] Du meng." Data security in cloud computing" in yhe proceeding of the The 8th International Conference on Computer Science & Education (ICCSE 2013) April 26-28, 2013. Colombo, Sri Lanka

[7] Hamid Banirostam, Alireza Hedayati, Ahmad Khadem Zadeh and Elham Shamsinezhad." A Trust Based Approach for Increasing ecurity in Cloud Computing Infrastructure" 2013 UKSim 15th International Conference on Computer Modelling and Simulation