International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 1, Jan-Feb-2021, ISSN (Online): 2395-566X

Identification of New Cloud Computing Approach for User Authentication and Protection

Research Scholar Nipun Sharma, Prof. Dr. Rohit Kumar Singhal
Dept. of CSE
IET Alawr

***Abstract*- Cloud computing is the very attractive technology area in the current era due to its cost effective, flexible and portable services. Cloud computing is basically a business model which provides services related to Information Technology on demand over network. It offers on demand network access to the pool of shared resources with minimal management effort and service provider interaction. When the services of Cloud Computing are used, the major issue arises, that is security. To tackle with these kinds of issues, Cloud Provider must have sufficient control to provide security. There are different-different provisions available with service provider to handle such kinds of above security issues. Intruders can affect files stored in the cloud or messages of users by intercepting. There is required to provide security to files or messages by means of encryption techniques.To prevent attacks like chosen plain text attack, chosen cipher text attack, denial of service attack.**

***Keywords:*- Software and its engineering, Software organization and properties, Software system structures, Distributed systems organizing principles.**

I. INTRODUCTION

Cloud Computing is defined as delivery of service rather than a product. Cloud computing is a model of storage, delivery and data processing in which actual resources are provided to the client on lease and on demand on pay for use basis.Cloud Computing has been defined by the NIST(National Institute of Standards and Technology) as:"Cloud Computing is a model for enabling convenient, on-demand network access to the shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort and service provider interaction.This cloud model promotes availability and is composed of five essential characteristics, three services models and four deployment models.

The general model of Cloud Computing mainly consists of Data Owner, Service Provider, users and communication channels. These components are communicating with each other continuous. If data owner wants to share any data, just send to the storage of Cloud. The users may access those data by sending request query to the Cloud. The Cloud or Service Provider authenticates the user or data owner and sends the data or reply back to the user or data owner. These configurable computing resources can be network, storage, server, application and services.The general model of cloud computing is shown in following figure.

The term "Internet Networking" is a fundamentally centralist ideology of communication and grid computing. Such researchers describe cloud based computing as the basis of dispersed grid based cloud computing refers to features and circumstances in which complete computation by anyone else, having different hardware and software, may be done utilizing the network.

Typically, the scattered nature of networks identified as customer clouds is typically distributed; nevertheless, this is not evident to consumers or might not be appropriate to explain this by way of cloud computing explanations. In recent years, the cloud has evolved from two different points of view-the leasing of a cloud network or the leasing of a specific cloud application. Where the former deals with the functionality or usage of web-based software, the latter is restricted to the "easy" products or services of cloud systems and providers. A number of terminologies have extended to the software sector, such as SaaS, PaaS (Platform as a Service) and IalyS

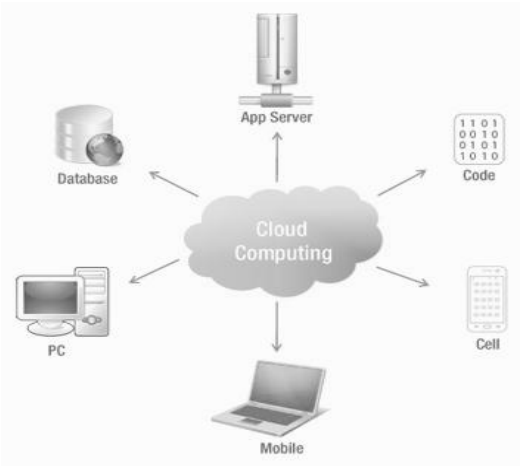

Fig 1. Cloud Computing General Model.

(Infrastructure as a Service). The word "internet computing" has a meaning, as previously stated and also defines numerous variants of cloud computing. In the wider sense, infrastructure may be defined as the devices and configuration inside the computer network, where the networks are a software operating system. Thus, cloud computing at the core of a network is only a specialized form of grid and cloud computing that has various networks, services, uses and geographic distribution The technical level defines how much a consumer "borrows" the methods from the device into the applications the degree of abstraction does not influence the main security questions and the measurement mode. This enables protection to be considered as part of all cloud storage platforms regardless of form, hierarchy and abstraction. In contrast to current cloud protection problems and storage issues, Virtualization is an unavoidable technology which is closely related to the idea of the cloud machine, which is part of cloud services particularly in the sense of PaaS and SaaS, and which is one of the physical networks 's resources.

II. CHARACTERISTICS OF CLOUD COMPUTING

Cloud Computing has some important characteristics which are as follows:

1. On Demand Self-Service:
A user can provision computing capabilities like server time, network storage resources as per its need and nearly instant access without human interaction with each service provider.

2. Broad network access:
The information and resources available on the network should be accessible from any location and by any heterogeneous structured devices or platforms like PDAs, Laptops, Desktops and Mobiles etc.

3. Resource Pooling:
Compute, Network and Storage resources are delivered to the user from a large pool of resources and different organizations with dynamically allocation as per user demand. This resource allocation must be location independent.

III.VIRTUALIZATION

In Cloud Computing, the services are provided through virtualization. Virtualization is a technique which creates multiple logical system from one physical system. Virtualization has two types, one Full Virtualization, in which complete installation of one machine is run on another machine. Second is Para-virtualization, in which multiple operating systems are running on single machine at the same time by efficiently using of system resources.

There are two types of virtualization found in case of clouds as given in:

- Full virtualization
- Para virtualization

1. Full Virtualization:
In case of full virtualization a complete installation of one machine is done on another machine. It will result in a virtual machine which will have all the software's that are present in the actual server. Here the remote data-centre delivers the services in a fully virtualized manner.

Full virtualization has been successful for several purposes as pointed out in:

- Sharing a computer system among multiple users.
- Isolating users from each other and from the control program.
- Emulating hardware on another machine

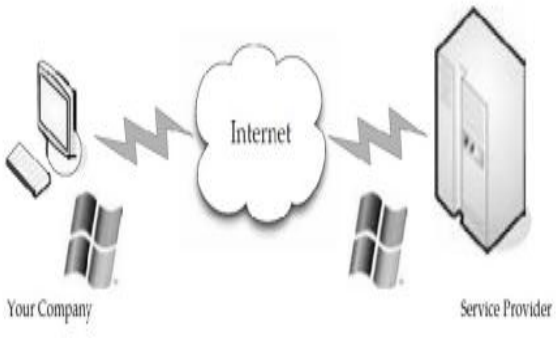

Fig 2. Full Virtualization.

2. Para Virtualization:
In Para virtualization, the hardware allows multiple operating systems to run on single machine by efficient use of system resources such as memory and processor. e.g. VM ware Software. Here all the services are not fully available, rather the services are provided partially.

Para virtualization has the following advantages as given in:

2.1 Disaster recovery: In the event of a system failure, guest instances are moved to other hardware until the machine is repaired or replaced.

2.2 Migration: As the hardware can be replaced easily, hence migrating or moving the different parts of a new machine is faster and easier.

2.3 Capacity management: In a virtualised environment, it is easier and faster to add more hard drive capacity and processing power.

2.4 Implicit grants: This method is used to give the recipient a consumer authorization token in computer language (Angry Birds app). Though implicit help reduces the overhead strategy, protection threats may be added.

2.5 Authentication grants to asset owners: A demand control key for this type of contract is provided with the credentials of asset owners (usernames and authentication). Such a subsidy will be provided if the receiver completely trusts the consumer.

2.6 Consumer password subsidies: This form of subsidy can be used to limit access to protected web services including Facebook user profiles.This can be done by keeping a database safe (Facebook Account Profiles) or by receiving authorisation from the provider (the Angry Birds app) to access the vulnerable information. The consumer (Angry Birds app) sends a license assignment to the Facebook server for entry to the card.

The resource server confirms the permission token (Angri-Birds application) and enables the client to permission its property. For examples, the business might post the accomplishments of the consumer on its Facebook schedule. ity vulnerabilities that arise from the Protocol (Google Developers, 2014) as Google implements OAuth 2.0 if OAuth's 2.0 is not implemented correctly. This specification is intended to integrate the Google API into database servers and implementations with the OAuth 2.0 protocol to be used by web server apps, including game apps. [41]

IV. THE PROTOCOL SPECIFICATION AUTHORIZING

1. Process works:
An example of an authentication mechanism to prevent DoS attacks on a standard network is the Host Identification Scheme (HIP). This feature cannot, however, be enforced in the application layer to defend against global DoS assaults. The fact that HIP is based on network layer host identification in the OSI reference model is illustrated. In addition, at the operating system level it is configured and controlled. In addition, any IP address identification security method, such as Internet Protocol Safety (IP Sec), cannot hide the identity of the participants.

Fernando, N., Loke, S.W. et.al, 2013 HIP is coping with the DoS-SYN flooding in the section with more processing to create the new TCP connexion between the two participants. The latest four-way handshake concentrates on an encoding challenge that allows the consumer to bypass a hash function. This helps a individual to perform such programming tasks using a puzzle solution mechanism. A simple server activity validates the puzzle response.

The restore token can be stored for offline access on a server's web applications for future communication data. The stored refresh token is unused before the device cancels. Such stored data may generate preventive faults to remove storage space from web servers as described. [43]

2. Authentication protocol validation:
The definition principle to include the security requirements of authentication protocols has already been suggested by Burrows, Abadi, and Need ham (BAN) and was later introduced by Sigerson and Van Oorschot (SVO) as a model extension to overcome other BAN limitations. Any of SVO's own remarks are close to those in BAN.

3. Premise:
Latest state declaration setup.

4. Assumption of the communication received:
To assume the communication obtained by the researcher through the usage of the procedure with any testing process that is positive and scientific. The Fig diagram is an example of procedures to authenticate the various But against DoS attacks, they 're not shielding. The authentication solution recommended the inclusion of the common username for shared and cloud infrastructure authentication. Although authentication allows replay attacks, DoS attacks are not supported. There are a number of DoS protocols that are used for cloud-based encryption evasion utilizing an intelligent card reader. Any programme authentication users may also use a card reader system.

Fig 3. Social authentication icons.

[Han, J., Susilo, W. et.al, 2013] [46] A number of vendors are actually operating the authorisation process (as OAuth), as seen in the Fig, as Facebook, YouTube, this protocol handles third-party customers 'connections to HTTP facilities.

Think, for example, about a customer trying to play Angry Birds and to update their Facebook page with videos and photos. In this situation, consumers have to include the Angry Birds software for their Facebook account to access player details and change game scores under their

consumer's name. Another example of a protocol that separately incorporates DoS Danger is a protocol that attempts to safely authenticate a key exchange between participants. In this protocol, the server starts calculating the exponential value when the first message is obtained and the address is produced. In the initial issues, the development teams are therefore overloaded.

5. Understanding reference:
An assumption regarding the recipient's opinions and the ambiguous dimensions of the received letter.

6. Interpretation inference:
Inference of how each group interprets the messages obtained. Derivation: the analysis goals shall be excluded from the premises above.

[**Ismail, N, 2011]** The combined usage of resources for the requester (user) and the respondent (server). [48] The estimation costs are specified as the overall use of resources. The damage is measured and minimized over the course of the operation before the DoS intruder is found. On each step used in authentication on the applicant's hand, net expense of the complainant is the cumulative expected expense before the authentication phase is terminated. In fact, the cumulative expense of any proceeding during the verification process is measured before the claimant determines that the claimant is either a legitimate applicant or an intruder.

Such possible vulnerability problems provide the ability to provide a password for accessing data storage. An attacker who first accesses the Public Cloud through a licensed password, computer or network will be allowed to access the data contained in the Cloud as Organizations also require an algorithm that can identify such criminal violations effectively.

In addition, other protection threats such as access for privileged users, position of data, data isolation as well as data recovery are likely to place cloud storage layers at risk. One of the levels of usage open to general users on the Internet is decentralized cloud computing. SaaS (Software as Infrastructure) is a standard application layer, in a similar sense, and can be used for the usage of public cloud data as an entry point. Via a website or a software interface SaaS can be accessed by potential users via password, anywhere and by using any app as it works to register and enable access to all users.

Trust is also a protection question for utilizing the cloud service because it is specifically connected to the reliability and quality of the delivery of the cloud service. Confidence may become the secret to a good cloud storage climate. Trust model provision in cloud computing is important, as this is a shared field of concern for all stakeholders in growing cloud scenario. Confidence in the cloud can depend on different factors, including technology management and human factors, processes and policies. Cloud confidence is not a technological protection concern, but the most significant soft factor is motivated to a large degree by the security problems of cloud computing.

VI. CONCLUSION

A key issue in this regard is the transmitting feature of other networking systems. The cloud system includes physical and computational capabilities which presents a variety of protection challenges at various stages. No advanced authentication method is a current cloud infrastructure challenge to completely resolve security threats.

The key consequence was the usage of grid computing as an important part of cloud infrastructure since the virtualized services are closely connected to a cloud network, protection considerations pertaining to penetration are critical for security issues.Throughout the operating context of a cloud storage system. it must be taken into consideration to be abused but cost savings and globalization patterns would force nearly all organizations to accept internet and connected innovations as the primary means for cloud computing.

In addition to the cloud-specific security issues, overall protection risks linked to the Internet are required to be immediately implemented. Another approach to keep cloud infrastructure versatile is to include portability. Cloud storage portability can often be related to security problems. Data portability helps web customers to migrate between multiple suppliers of cloud service by modifying the ways they execute activities in a number of ways. It is evident that cloud consumers are able to leverage power; however, safety problems with cloud portability need to be resolved at the same time.

Web portability can pose severe security threats centered on APIs the rapid shift to mobile computing activities has rendered mobile computing and its related technology a critical component of cloud computing available in recent years. Scarcity of infrastructure and other mobile networking limits become cloud computing hurdles.

REFERENCES

[1] “A survey on security issues in service delivery models of cloud computing”, S. Subhasini, V. Kavitha (2010), Journal of Network and Computer Applications, Pages 1-11.
[2] “Anonymus And Fuzzy Identity Based Encryption”, P.P. Van Liesdonk (2007).
[3] “Secure Key Issuing in ID-based Cryptography” ,Byoung cheon Lee, Colin Boyd, Ed Dawson, Kwangjo Kim, JeongmoYang, Seungjae Yoo.

[4] "A Survey on ID-Based Cryptographic Primitives",M. Choudary Gorantla, Raju Gangishetti and Ashutosh Saxena.
[5] K. Vieira, A. Schulter, C. Westphall, C. Westphall (2009), Intrusion Detection Techniques in Grid and Cloud Computing Environment, IT Professional, IEEE Computer Society.
[6] "Determining Service Trustworthiness in InterCloud Computing Environments", J.Abawajy (2009), 10th International Symposium on Pervasive Systems, Algorithms, and Networks,Pages 784 -788.
[7] Kamara, S., Lauter, K.: "Cryptographic cloud storage" In Proceedings of the 14th international conference on financial cryptography and data security, FC'10, pp. 136-149. Springer-Verilog, Berlin, Heidelberg (2010).
[8] Wang, C., Wang, Q., Ren, K., Lou, W., "Privacy-preserving public auditing for data storage security in cloud computing"2010 Proceedings IEEE INFOCOM 54(2), 1-9 (2010)
[9] Joshi, K., Yelena Yesha, and Tim Finin. "Automating cloud services life cycle through semantic technologies."2012.
[10] Blanchet B. "An Efficient Cryptographic Protocol Verifier Based on Prolog Rules" In Proc. 14th IEEE Computer Security Foundations Workshop (CSFW), pages 82–96, Cape Breton, June 2001. IEEE Computer Society.