International Journal for Innovative
Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 5th Jan 2021. Link :http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=ISSUE-01

DOI: 10.48047/IJIEMR/V10/I01/01

Title: **LOW COST ROBUST SERVICE OVERLOADING FUSION MODEL FOR CLOUD ENVIRONMENTS**

Volume 10, Issue 01, Pages: 1-8

Paper Authors

Ramesh Vishwakarma ,Dr. Sitendra Tamrakar ,Dr. Rishi Kumar Sharma

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

LOW COST ROBUST SERVICE OVERLOADING FUSION MODEL FOR CLOUD ENVIRONMENTS

[1]Ramesh Vishwakarma ,[2] Dr. Sitendra Tamrakar ,[3]Dr. Rishi Kumar Sharma
[1]Research scholar in RNTU,Rabindranath Tagore University ,Bhopal, India
[2]Associate Professor, Nalla Malla Reddy Engineering College, Hyderabad,India
[3]Assistant Professor (CSE),Scope College of Engineering ,Bhopal ,India

Abstract

The integrity security of the data is a most important issue on cloud environment as it is directly related to the cloud end user. Since all the cloud data services are derived by Internet, data security (DS) is a biggest problem in cloud. Security of data involves various risks and the proposed SOFM model will address the security issues of the secure data transaction on cloud environment. For secure data transmission (sending & receiving) over cloud environment, a security layer has been implemented between the Base overloaded cloud end and derived cloud server. A new scheme includes service exchange has been implemented to provide the intended security in the environment and to mitigate those security risks respective to the cloud consumers. Existing technique have been improved for the designing of the proposed model. It makes the service overloaded cloud server (OCS) and provides a secure cloud environment. The proposed SOFM scheme has provided preferable security and improved the performance than any other existing key management technique.

Keywords: Cloud authentication, computation, low cost authentication.

I. NTRODUCTION

Cloud Computing is the new technique of creating and providing on-demand computing services. The cloud services include everything from applications to datacenters over the network and on the pay-per-use (cloud consumer) basis . Cloud Computing is also oftentimes referred to as “Cloud” or “cloud to Cloud” [1].The whole process of creating and delivering computing services adds competitive value to business, operation, and innovation; however, security concerns are among the leading barriers to the Cloud adoption. These security concerns cause the trust problem [3, 11] in the Cloud.

Using this theoretical data like execution complexity, types of network attacks, Wireless(cordless)-Local-Area-Network (WLAN) security, advantages and disadvantages isn’t sufficient to choose a distinctive authentication method. So, an experimental network analysis is required to choose a cloud security for authentication, which gives preferable performance in terms of secure authentication time and (TPT) total processing time. This prompt us to evaluate the network performance of widely used cloud security techniques for both wired and wireless networks. We calculated two parameters namely; communication cost and authentication time.

In the real world it is compulsory to compare the scalability of both wireless and wired cloud networks. This scalability will give us the information if same protocol can be used for both wired network and wireless cloud network, or apart protocols needs to be used for wireless and wired networks.

II. CLOUD COMPUTING ENVIRONMENT SECURITY ISSUES

In the last ten years, cloud technology has growing from being a promising data and information security problem and business notion to one of growing area of IT industry.. This research section highlights the security problems and requirements that stem from the characteristics of cloud computing environment and gives a technical description of the most relevant attack scenarios.

Reliable Service and secure data availability: Secure network reliability is a key cornerstone for cloud computing environment and cloud services. Because a cloud is accessed over public local networks , cloud provider must point out the probable for loss of Internet network backbone connectivity. The common problem should be a main consideration for cloud service user who entrust infrastructure to cloud. Availability is also a main problem for private cloud infrastructures.

Security: Where is your data and information more secure] on your local storage (personal storage) or on security servers in the cloud environment? Some argue that user information is more secure when managed inside] while others infer that cloud providers (SP) have a strong stimulus to maintain faith and as such employ higher security- But] in the cloud environment] your data and information will be spread over these individual computers regardless of where your base repository of data is ultimately stored- Attacker can attack virtually any local server or cloud server] and there are statistics that]show that one-third (OT) of breaches result from stolen laptop and other devices and from employees* accidentally showing data on the Internet] with nearly 16 % due to insider theft-

Privacy : The cloud computing make use of the virtualization technology] cloud users* personal data and information may be outspread in many data center (DC) rather than stay in same location, even across international borders] at this time] data and information privacy protection will face the dispute of different legal systems- On the other side] cloud customers may leak hidden information or data when] they accessing (use) cloud services- Cloud attackers can analyze task depends on computing task submitted by the cloud users-

Cost-effectiveness: One of the key factors used by CSP to promote their solutions is that they cost less than acquiring whole software/ hardware architecture.

III. FUSION MODEL

Cloud is a service field .The matter of fact that cloud can propose both storage and computation at low cost amounts makes it popular . This also develop it a very useful and powerful proposition for the future. But in spite of its potential, security in the cloud proves to be a cause for concern to the data security sector. These security concerns also make the use of cloud services less flexible. In this research model work, we represent a secure service overloading Fusion Model that permit data to be stored securely in cloud while at same time allowing operations to be performed on it without any compromise of the sensitive parts of the data.

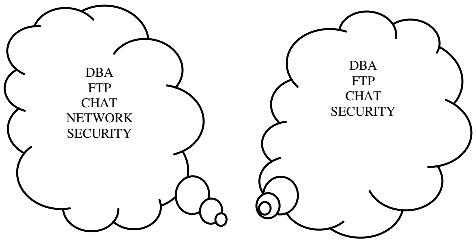


Fig. 1

Cloud has characteristics and associated behavior- A bring service can see which is its behaviors. But its behavior may differ in different situations. The key of cloud overloading is a cloud’s services list which is also known as the service overloading signature. It is the signature not the type that enables cloud overloading.

If tow cloud are having same number and type services in the same order, they are said to have the same signature and if they are using distinct services name, it does not matter. Even if they are using distinct network.

To overloaded a cloud name, allow need to do is declare and define all the cloud with the same name but different signature separately.

The user ID and Service type of determine which cloud should be invoked. A cloud called first matches the OTP available service type provide with the cloud call and then calls the appropriate cloud execution , Cloud overloading is a logical method of calling sever as cloud with different services and services type that perform basically identical thing by the same name. Cloud overloading a service name provides the services with same name having different signature. To overload a services name, all we need to do is, declare & define all the functions with the same name but different signature, separately.

The previous research described several security issues impacting the cloud computing model and authentication. The security state of cloud computing is still puzzling. It shifts computing perceptions entirely from the customer viewpoint, outsourcing IT systems instead of adopting local solutions. Authentication is also being subject to changes. The static one-factor login is no longer viable. Systems are often vulnerable to data breaches, and attackers are increasing their arsenal of tools and techniques for brute-forcing password hashes, gradually lowering trust of password usage. As such, research on authentication is focused on augmenting existing mechanisms or utilizing QR encoding, SMS messages, OTPs, or biometrics based on growing mobile technology for devising novel MFA approaches, while aiming to achieve important security properties like perfect forward secrecy and completeness. Nonetheless, little attention is payed to the underlying infrastructure, and few have looked into harnessing the cloud computing technology for the purpose of making authentication more robust, in response to the adversity of Internet threats to public clouds, particularly to the management interfaces.

CLOUD OVERLOADING

Cloud has characteristics and associated behavior. A bring service can see which is its behaviors. But its behavior may differ in different situations. The key of cloud overloading is a cloud's services list which is also known as the service overloading signature. It is the signature not the type that enables cloud overloading.

If tow cloud are having same number and type services in the same order, they are said to have the same signature and if they are using distinct services name, it does not matter. Even if they are using distinct network.

To overloaded a cloud name, allow need to do is declare and define all the cloud with same name but various signature separately.

Cloud overloading a service name provides the services with same name having different signature. To overload a services name, all we require to do is, declare & define all the functions with common name but different signature, separately.

SERVICE OVERLOADING

Service overloading provides a way to define and use services such as upload, download and for user defined type such as cloud and security services .Let's develop a "overloaded "cloud to illustrate the user a utility of services overloading.

Cloud overloading allows any of its built in service to be overloaded in a cloud but only those that have an intuitive meaning for a particular cloud should actually be overloaded.

Cloud overloading is one of the most challenging and exciting characteristics of cloud. Service which already exists in the cloud can only be overloaded. Overloading can't alter either the basic template of a service, nor its place in the order of precedence. Service overloading can be carried out by means of either based cloud or drive cloud.

If any clouds have multiple services with same names but different parameters time (PT) then they are said to be overloaded. Service overloading allows you (user) to use same type name for different range, to perform, either same or different service in the same cloud network.

IV. IMPLEMENTATION AND RESULTS

Simulation Environment

The cloud sim simulation environment is created by composing four components; two overloaded Cloud, and two clients, all the four components are implemented on computers having P4 3.0 CPU, 2GB RAM. The service overloading technique implements on the equal all clouds.

As shown in Fig.2, the communication cost of SOFM is approximately 1526 bytes while that of APCC is 1588 bytes.I want to say that, the data communication cost of SOFM is 96 % of that of APCC.

Table 1. Comparison of communication cost

S No.	Location	APCC	Location	SOFM
1	Lab	1582	Europe	1530
2	Lab	1583	Arab States	1520
3	Lab	1585	Africa	1510
4	Lab	1588	Asia	1515
5	Lab	1589	North America	1525
6	Lab	1592	South/Latin America	1510
7	Lab	1589	Arab States	1525
8	Lab	1594	North America	1580

Fig.2 Comparison of communication cost

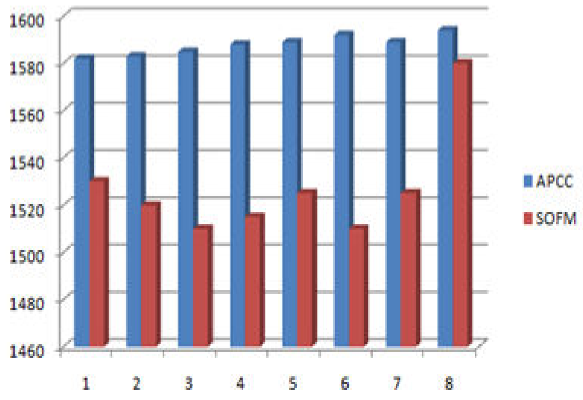
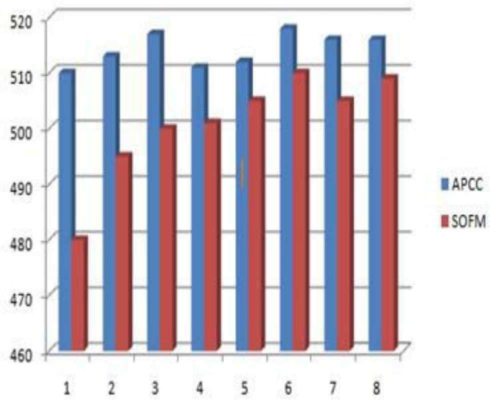


Fig.3.shows in the authentication time of SOFM is approximately 500 ms while that of APCC is 514 ms .That is, the authentication time of SOFM is 97% of that of APCC. The simulation authentication time results homologate that the communication cost of SOFM is lower and authentication results time is shorter.

Table 2 Comparison of authentication time

S No.	Location	APCC	Location	SOFM
1	Lab	1582	Europe	1530
2	Lab	1583	Arab States	1520
3	Lab	1585	Africa	1510
4	Lab	1588	Asia	1515
5	Lab	1589	North America	1525
6	Lab	1592	South/Latin America	1510
7	Lab	1589	Arab States	1525
8	Lab	1594	North America	1580

Fig.3. Comparison of authentication time



In APCC, each virtual node has a unique name. This technique work with multi-level (ML) but proposed technique (SOFM) overloaded]service or generate an environment and perform the task, hence the proposed technique (SOFM) takes less authentication time and computations hence SOFM is better as compared to APCC.

V. CONCLUSION

The proposed model has been designed to overcome the problems of the security during the data transmissions over the cloud network- The proposed model offers the effective key management scheme for the purpose of link security and encryption for the purpose of data integrity- The proposed model has been clearly outperformed the existing work compare in. In this research work, the implementation of Cloud overloading Technique and its analysis is given. The service overloading technique can provide quick and secure access to cloud services under the cloud security environment even when users are in motion. Compared to the conventional service overloading technique this authentication process does not require to carry any device always and there is no cost for purchasing or replacing any hardware and can provide easy access to the cloud service with convenient authentication process. Finally the proposed study has proved its superiority over SOFM and APCC techniques.

REFERENCES

[1] J. Karlin, S- Forrest, J- Rexford, "Autonomous Security for Autonomous Systems," Proc- of Complex Computer and Communication Networks, Vol. 52, Issue. 15, pp. 2908- 2923, Elsevier, NY, USA, 2008-

[2] M. Jensen, J- Schwenk, N- Gruschka, and L- Lo Iacono, On Technical Security Issues in Cloud Computing. IEEE, 2009-

[3] http://www.cloudsecurity-org, accessed on April 10, 2009-

[4] J- Hu and A + Klein] "A benchmrk of transparent data encryption for migration of web applications in e cloud]" 8th IEEE Int- Symp- Dependable, Auton. Secur. Comput. DASC 2009, pp- 735–740, 2009-

[5] D- Descher, M., Masser, P-, Feilhauer, T-, Tjoa, A-M- and Huemer, "Retaining data control to the client in infrastructure clouds," Int- Conf- Availability, Reliab- Secur- (pp. 9-16) - IEEE., pp. pp. 9–16, 2009-

[6] R- Wei and Z. Zeng, KIST: A new encryption algorithm based on splay, IACR Cryptology ePrint Archive, 2010-

[7] Alain Bertrand, Bomgni, and Myoupo Jean Frédéric- "An energy-efficient clique-based geocast algorithm for dense sensor networks- "Communications and Network 2010 (2010) -

[8] P- Mell and T- Grance, “Draft Nist Working Definition of Cloud Computing,” http://csrc.nist.gov/groups/SNS/cloud computing/ index.html, Jan- 2010-

[9] K- Ruan, J- Carthy, T- Kechadi, M- Crosbie] “Cloud forensics% An overview,” 7th IFIP International Conference on Digital Forensics, USA, 2011-

[10] T-H- Cheng, Y-D. Lin, Y-C. Lai, P-C. Lin, “Evasion Techniques% Sneaking through]Your Intrusion Detection@Prevention Systems]” IEEE Communications Surveys & Tutorials, Issue 99, pp. 1-10, 2011-

[11] J- Srinivas, K. Reddy, and A- Qyser, “Cloud Computing Basics,” Build- Infrastruct- Cloud Secur-, vol. 1, no- September 2011, pp- 3–22, 2014-