Four Dimensional Security and Vulnerability Matrix for Cloud (4-SVM)

On the arena of Cloud ERP

Sharmistha Dey
Assistant Professor, IMS Ghaziabad
Ghaziabad, India
Email: sharmistha.dey@imsgzb.com

Dr Santanu Kumar Sen
Principal ,Guru nanak Institute of Technology
Kolkata,West Bengal, India
Email: profsantanu.sen@gmail.com

***Abstract*—Cloud computing is a catchphrase for today's ICT world. The emerging trend of "Everything as a service" has made this rapid growing technology a very admired and highly demanding technology for a must adapted one. With the virtues of 24x7 service availability, multi tenancy, utility, speed, high productivity, agility, scalability of this technology, it has been proved as an emerging trend for the ICT industry as well as the academia. Today the rapid data analytics is changing the way companies try to win, and hence enabling them to generate instantaneous insights for supporting their most important business processes.**

In present technological era, cloud combining with IOT or Big Data, or highly popular commercial ERP solutions, namely SAP cloud, has touched the height of technological growth but one of the major reasons for the trepidation of its widespread adaptability is the security and authentication breach in cloud technology. Being used in highly commercial solutions, the security issues play a major role.

Threat or vulnerability is more important to qualify rather than being quantified only. This paper is a proposal showing a quantifiable approach, focuses on several threats and security breaches and countermeasures their impact concentrating on a cloud based solutions, with the philosophy of the inevitability of testing on cloud security.

***Index Terms*—Alpha Reliability, Cloud ERP, Distributed DOS, ICC, ROTA, SLA.**

I. Introduction

As per the NIST draft, Cloud computing is a unique model for enabling ubiquitous, suitable, on-demand network access to a common pool of configurable resources for computing (such as networks, printers, servers, storage devices , applications, and other services), that can be hastily provisioned and can be released with nominal management effort or communication with the service providers [9].

There are mainly three basic cloud service types – Public cloud, private cloud and Hybrid cloud and several deployment models for cloud namely mobile cloud, community cloud etc.

This highly emerging technology has so many dimension that industry as well as the academia personnel can never vacillate to approve this technology. But the main concern about cloud service is when users reposition their services from their own IT infrastructure and the services are being prohibited by a third party cloud vendor, the vendor should be a dependable and trustworthy one. There is no such checkpoint in that area which can individually determine the efficiency and productivity of the cloud service that the company want to adopt.

This paper focuses on some significant threats and vulnerabilities of cloud with an analytical approach.

II. Recent Attacks On Cloud

Several attacks in cloud is the most noteworthy matter of concern today, which are coming using some attack vectors, which is known as a route or path using which the invader can be able to make a malicious entry into the system. They take advantage of some known weak spots for entering into the system [5-6].

According to a report from Cloud Security Alliances, the top thirteen threats for cloud in 2016 are as following [5]:

1. Data Breaches
2. Weak Identity, Credential
3. Access Management
4. Account Hijacking
5.System and Application Vulnerabilities
6. Insecure APIs
7. Data Loss
8. Advanced Persistent Threats (APT)
9. Nefarious Insiders
10. Insufficient Due meticulousness
11. Denial of Services
12. Abuse and Nefarious Use of Cloud Services
13. Shared Technology Issues

Many intruders are willing to take benefit of the human elements in the system, because they are generally the weakest link. Emails and their attachments via emails can cause the deception. Even though some intruder doesn't make an attack directly, lack of knowledge and credulity , due to which the system is being attacked by multiple nefarious people.

***i) Denial of Service (DoS) attacks**:* This popular attack is a widespread network level attack launched by a harmful intruder in which the hackers intentionally flood a network server with recurrent request of services with an idea to injure the network; make the server so much busy that it could not legitimate clients' normal requests of the services and become unavailable. In cloud computing, the attacks on the server happen by sending a huge number of requests to the server, and hence the server becomes unable to respond to the standard clients. The server will be disrupted from working normally. In Figure 1, a picture for the Denial of service attack has been illustrated; using a zombie network the attacker spreads attacks to the further level.

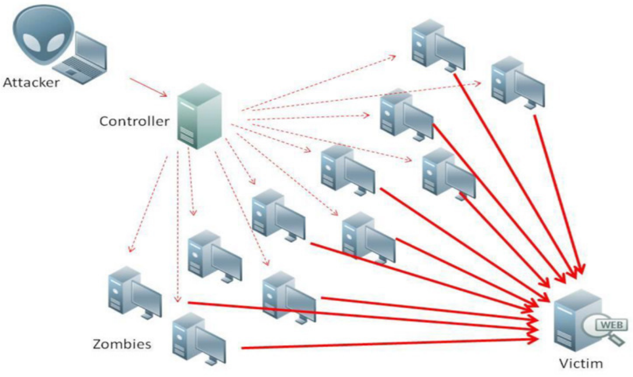

Figure 1: Denial of Service Attack

ii) Cloud Malware Injection Attack – This attack happens when a client opens an account under a cloud vendor, the cloud service provider generates an image of the customer's Virtual System in the cloud image repository system. In case of this attack, the invader takes several challenging attempts. Actually the attacker inserts malevolent service or code, which appears as one of the applicable instance services running in the cloud. If the attacker will be successful, then the cloud service will suffer from the problem of eavesdropping [12-14]. The key idea of this attack is that an invader uploads a manipulated copy of victim's service by injecting their own malicious codes and this attack is a major ambassador to exploit the service-to-cloud environment [12-15].

iii) Distributed Denial of Service Attack (DDOS Attack) **-**This is an extended DoS attack in distributed platform where several systems are compromised and used to build the zombie network, they are generally contaminated with a Trojan Horse and used to target a single system declaring a Denial in the Services. Victims of a Distributed DoS attack may face attack from both end compromised network behaving as a zombie as well as from the master attacker.[14]. The eavesdropper act as a master component, he launches rigorous attacks on the victim, via a compromised distributed network which is again separated into different compromised layers of network .

iv) Side Channel Attack – This happens within a piece of hardware having numerous virtual resources , which in turn are shared and they can act as a side channel data from one virtual system to another. Those attacks are based on the shared resource victimized by the attackers.

v) Cross Site Scripting Attacks –This is also known as XSS attack, which may be treated as a security breach, where the eavesdropper inserts malevolent codes into a link which appears to be from a dependable and trustworthy source. After clicking on the link by the victim, the entrenched programming will be submitted as a part of the client's request and the whole thing will be executed on the user's computer, This kind of attack allows the attackers to take information without the awareness of the user. So, as an alternative, it will be directed to the harmful site instead of going to the original site. This attack has a major impact on cloud services. [14-15].

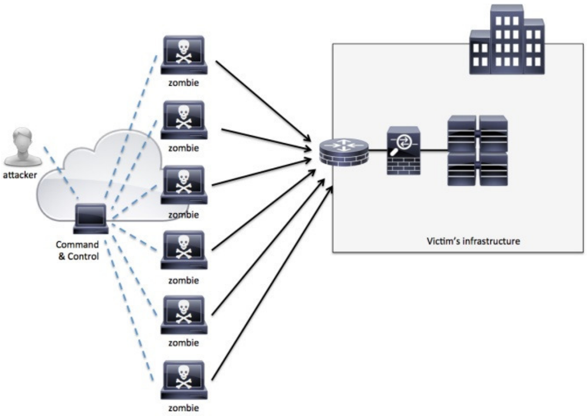

Figure 2:Distributed Denial of Service Attack

vi) v) Insecure API-Now days**,** Attackers have begun to aggressively target the digital keys which are being used to secure the internet infrastructure. The unidentified attackers can steal important information on RSA's SecureID token, making the API unreliable.

III. Related Background Study

There are many significant contributions in this area. For a few years scientists are working on this emerging field. Dr G. N. Purohit and et al, in their study, entitled as "Challenges Involved in Implementation of ERP on demand solution : Cloud Computing ", has highlighted the special issues related to Cloud ERP solutions as this is the highly commercialized one and important on account of Business perspective[8]. In another study, "Competition and Challenge on Adopting Cloud ERP", the authors Fumei Weng and Ming-Chien Hung has clearly stated how beneficial cloud is for ERP system and why the professional services like ERP needs Cloud is willing to adapt the ERP service[9]. The ontology of cloud computing has been defined very ornately in their study. The particular structure of security risk has been made prominent and there are many methods for avoidance of those attacks upon cloud. The target can use diverse methods to intercept data sent by a malicious user. In an another survey paper entitled as, "Study of Cloud based ERP service for small and medium enterprises", author Rajeev Sharma and Bright Keshwani have confirmed significance of the several security issues faced by Cloud ERP, specially for small and medium scale industry[10][14-15]. The security guidelines for Cloud ERP service, provided by SAP, have been clearly formed out. The General Terms and Conditions (GTC) for SAP Hana cloud shows a clear discrimination with other SAP models which are not using cloud. The distributive nature of the system has made it more attack-prone[19].What are the major terms for handling SAP and the main responsibilities has been pointed out in that article, which in turn works as a support for the proposal to establish a relation.

IV. Proposed Work : 4-Svm Matrix For Cloud

Today cloud security is being treated as an elementary issue for adaptability of different cloud service , from both end, from the viewpoint of providers as well as the users. In this paper, an innovative concept of four Dimensional Security and Vulnerability Matrix (4-SVM) has been proposed keeping several network aspects in mind, where the authors have proposed a neutralize quantization of quality of cloud services, with respect to four aspects- availability, reliability , Integrity and confidentiality- a multidimensional and mathematical matrix model have been formalized for computational easiness and strictly based on some cloud security measuring points as parameters of the matrices. Most important objective of the proposal is primarily identifying different types of possible attacks including traditional as well as specialized attacks, then it will measure the impact of different types of attacks with suitable and reasonable metrics with some mathematical formulas and questionaries.

Cloud combined with ERP tends to a less secure one causing some extra headache for the developers and service providers. The proposed model can measure the impacts of those attacks, for a special case, Cloud ERP system has been considered. The strategic goal of this system is to convert weakness into strength by measuring the impact of various threats on cloud and quantifying the quality of Services[6-9][14-16]. The proposed four matrices are as follows :

1. Confidentiality Matrix(CM)
2. Integrity Matrix(IM)
3. Availability Matrix(AM)
4. Reliability Matrix (RM)

Loss of Confidentiality in cloud may straightly be related with the Asset in term of both tangible as well as intangible.

In financial accounting, **assets** are known as mainly the economic resources, which may be tangible or intangible, competent enough of being owned or prohibited to construct value and held to have positive economic value. In case of cloud ,especially when people consider the SAP Cloud which is a highly commercialized service , the asset loss can be measured by Return on Total Asset (ROTA), TA index measurable in terms of finance management, the formula of which is quite common for the commercial persons.[1].

Here, TA means Tangible Asset.

Lost TA Index=ROTA of Company / Loss of TA of company due to attacks against confidentiality

Confidentiality Matrix=

$$\begin{pmatrix} \text{Lost TA Index} & \text{Strength of Identity Provisioning} \\ \text{NROSI Index} & \text{Strength of Communication Security} \end{pmatrix} = \begin{pmatrix} wf1 & wf2 \\ wf3 & wf4 \end{pmatrix}$$

Figure 3: Confidentiality Matrix

Where, ROTA is Return on Total Tangible Asset. It is a ratio to measure a company's earnings before interest and taxes (EBIT) against its total net assets.

To measure this ROTA we have to do the following,

ROTA=EBIT/Total Net Asset, where EBIT=Net Income+ Interest Expense +Taxes

After measuring the value using those parameters, we can apply fuzzy logic to determine the probability of the ranges of value, which will be known as a weight factor. This weight factor can be a significant value for the scalability with response to asset loss due to some threats. Suppose, for a cloud ERP, you have imposed a security investment , then you can expect which return and how much return should be exempted due to certain vulnerabilities in the system, this can be measured by Non ROSI[21].

Security investment risk can be measured as :

Non-ROSI (NROSI) Index=1/ROSI

Non-ROSI (NROSI) Index=1/ROSI

$$\textit{Where, Return on security investment (ROSI)} = \frac{\textit{Risk}}{\textit{Exposure x \%of risk mitigated} - \textit{solution cost}}$$

Figure 4: Non-ROSI Determination

Strength of Identity Provisioning checks how system generates Identities while accessing data. The strength of the password is measured, whether It is an encrypted password or graphically encrypted password or single one[5].

While measuring the **Strength of the communication Security**, the system mainly has to measure the strength of the Encryption Key used. The strength of encryption algorithm will develop this factor. Complexity of the encryption algo that has been used to encrypt could be measured and again this can be put in a range.

Though the work is still in the proposal stage and not being populated with sample analysis , but the process is ongoing.

Integrity Matrix

$$\begin{pmatrix} \text{SLA Standardization Error} & \text{Strength of the hash function Used} \\ \text{Information Integrity Check Strength} & \text{Physical Security Hazard} \end{pmatrix} = \begin{pmatrix} wf1 & wf2 \\ wf3 & wf4 \end{pmatrix}$$

Figure 5: Integrity Matrix

SLA Standardization Error: The Service Level Agreements for cloud are very important. Therefore, it is a parameter, which can measure errors with respect to rate the Service Level Agreements(SLA). A cloud system should retort the agreements in time, unless it will be a vulnerable one. This parameter will measure the service level agreement conditions in terms of their acceptability or avoidance or deviation and again using fuzzy set it the model can be able to determine the impact factor for this standardization error [12].

Strength of Hash Function Used- This parameter could be able to take count on violation in the encryption algorithm has been used by the service providers and check the strengths for the hash functions used, whether it is MD5,SHA1 or SHA3. It will check the bit length and with known formula can be able to determine the type of hash function and hence it's strength. In case of SAP Hana Cloud generic hash functions with minimum 512 bits key length are being used nowadays. So this parameter will take the bit length as input and determine the effectiveness of the hash function, which is an important part in security.

Physical Security Hazard This parameter shows the difficulty faced by the placement of a physical server. It will take some questionnaires like in which location the server may be present probably, how many layers of security has been imposed to protect the server etc. and on the basis of those data it can determine the hazard a SAP Cloud user may have to face due to lack of physical security of a server.

The Availability Matrix is nothing but calculation of the availability of a service which has been measured by a very popular and well known method as follows :[Source- Rajib Mall, Software Engineering, 6th Edition]. The uptime and downtime may be taken as inputs.

$$\text{Availability} = \frac{MTTF}{MTTF+MTTR}$$

Where, MTTF=Mean time to failure and MTTR=Mean time to recovery

In case of ERP combined with Cloud, the availability is a very significant point. The clients have to give there input as uptime and downtime on a scheduled basis and hence this parameter will be able to count on a measure for service availability. Again applying the probability, we can determine the availability.

Reliability is the degree to which an assessment tool produces stable and consistent results. Poor reliability reduces the accuracy of a single measurement and it also decreases your ability to make a roadway for measurements.

The Reliability Matrix can be determined as:

Reliability Matrix

$$\begin{pmatrix} \text{ICC} & \text{Alpha Reliability Checking coefficient} \\ \text{Threat Responsiveness} & \text{Ease of Recovery} \end{pmatrix} = \begin{pmatrix} wf1 & wf2 \\ wf3 & wf4 \end{pmatrix}$$

Figure 6: ReliabilityMatri

ICC (Intra class correlation coefficient) is a measure of the reliability of measurements . Suppose the vendor has rated a cloud service. This parameter will crosscheck the rating. Two or more rater will rate this and the statistical probability of their rating will be taken for granted. Different rater will rate a service. Using soft computing, their confidence for a poll and reliability range will be determined.

Alpha Reliability Checking Coefficient is a new approach which is consequent and determined by assuming each item represents an acceptability of the reliability test. If there are five items, then five scores are the retest scores for one single item. However, the reliability is calculated with mean of the After getting the datasets, using SPSS analysis the alpha reliability can be rechecked.

Threat responsiveness This parameter shows how quick a system could be intelligent enough to response to a threat. These will be listed and will be used as an input to determine how much attack prone a system could be. A Cloud ERP can be traceable in terms of its responsiveness.

Ease of recovery This proves the criticalness of the threat. This factor can be determined by calculating maximum tolerable downtime(MTD), Recovery Time objective(RTO) and work recovery Time(WRT) as follows :

$$MTD = RTO + WRT$$

Depending upon the calculation the recovery easiness can be under the following categories :

- **Mission-Critical —from 0 to 12 hours**
- **Vital — from 13 to 24 hours**
- **Important — from 1 to 3 days**

- **Minor — more than 3 days**

In this way they can rank the reliability of a service.

From the above factors we can come to a solution about the trustworthiness of the system.

V. Conclusions And Future Works

Though cloud is not a latest technology for nowadays and researches in this field has become more mature in these days, still it leaves a plenty scope for the cloud researchers in this area as the independent tools for quantitative measurement of the impact of different security aspects are not quantified still now. Threats could be determined proactively and suitable countermeasures could be also taken. Due to lack of data required to analysis, this proposal is still now at the beginning stage, but the survey has been started and questioniaries have been formed for practical projection of the proposal and further research is going on to establish relation among the parameters. The prerequisite for identification, classification and accurate measurement of the maliciousness of those threats is primarily essential for the cloud providers using appropriate parameters which can analysis the effectiveness and trustworthiness of a cloud Service, specially highly commercialize service like Cloud ERP, which is a quite new one in these fields.

A lot of research scopes is still there in the specified field and our future goal is to give more focus on the parameters of the matrices which will develop a decision making tool using which could make the system more adaptable, smart and approachable.

References

[1] Santanu Kumar Sen,Sharmistha Dey,Debraj Roy, " Design of Quantifiable Real-Life Security Matrix for Cloud Computing",International Journal of Engineering Sciences and Research Technology, 3(5): May, 2014

[2] Ajey Singh, Dr. Maneesh Shrivastava "Overview of Attacks on Cloud Computing" published on International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.

[3] Sagar Tirodkar, Yazad Baldawala, Sagar Ulane, Ashok Jori, "Improved 3-Dimensional Security in Cloud Computing", International Journal of Computer Trends and Technology (IJCTT), Volume 9, Number 5, March 2014

[4] B. Meena and et al., " Cloud Computing Security Issues with Possible Solutions", International Journal of Computer Science and Technology, 3(1), Jan. - March 2012.

[5] Kazi Zunnurhain and Susan V. Vrbsky, Department of Computer Science,The University of Alabama, "Security Attacks and Solutions in Clouds"

[6] "The treacherous 12-Cloud Computing Top Threats in 2016" , Draft published by Cloud Security Alliances, February 2016

[7] Nielsen, Fran. "Approaches to Security Metrics." NIST and CSSPAB Workshop, Washington, D.C., 13-14 June 2000

[8] Dr. G. N. Purohit, Dr. M. P. Jaiswal, Ms. Surabhi Pandey, "Challenges Involved in Implementation of ERP on demand solution : Cloud Computing", International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012

[9] Fumei Weng and Ming-Chien Hung, "Competition and Challenge on Adopting Cloud ERP",International Journal of Innovation, Management and Technology, Vol. 5, No. 4, August 2014

[10] Rajeev Sharma, Dr. Bright Keswani , "Study of Cloud based ERP service for small and medium enterprises", Revista de Sistemas de Informação da FSMA n. 13 (2014) pp. 2-10 (ISSN : 1983-5604)

[11] P. Mell and T. Grance, "Draft NIST working definition of cloud computing - v15," 21. Aug 2009

[12] Resse, Mather,"Cloud Application Architecture Building Applications and Infrastructure in the Cloud", SPD O'Reilly publication, 2009

[13] Eyad Saleh, Christoph Meinel, " HPISecure: Towards Data Confidentiality in Cloud",13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing, Autumn 2013

[14] Meena,S, Daniel,E, "Survey on various data integrity attacks in cloud environment and the solutions", International Conference on Circuits, Power and Computing Technologies (ICCPCT), 20-21 March, 2013

[15] Sagar Tirodkar, Yazad Baldawala, Sagar Ulane, Ashok Jori, "Improved 3-Dimensional Security in Cloud Computing", International Journal of Computer Trends and Technology (IJCTT), Volume 9, Number 5, March 2014

[16] Stevenson, "Cloud Security and Privacy", SPD O'Reilly, 2010

[17] Mohit Mathur, KLSI, "Cloud computing Black Book", Wiley, 2012

[18] Wilder, "Cloud Architecture Patterns", SPD O'Reilly, 2012.

[19] Geneal Terns and Conditions for SAP Cloud ("GTC"), enEG.v.8-2016, A Whitepaper released by SAP Labs

[20] First Report on Security Metrics and Assessment-"Enforceable Security in the Cloud to Uphold Data Ownership", Swiss State Secretariat for Education, Research and Innovation , European Union's Horizon 2020 research and innovation programme, January 2015 – December 2016

[21] Wes Sonnenreich, "Return On Security Investment (ROSI): A Practical Quantitative Model", Sage Secure, LLC, NewYork,2006