International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

DESIGN AND DEVELOPMENT OF A REAL-LIFE SECURITY MATRIX FOR CLOUD COMPUTING

Santanu Kumar Sen, Professor;   Sharmistha Dey, Assistant Professor

Abstract

Cloud security has been evolved as a significant research area under the arena of information security that consists of network security and data security, and the area is not restricted to researchers only but also for the sake of cloud providers and users as well because of its tremendous potentiality towards flexible storage capacity, power of virtualization, multi-tenant features and highly commercial viability among the service industries, academia and others. However, the technology of concern, though possess lots of advantages, is all but free from some serious drawbacks relating to privacy and security issues, which are equally important for its wide acceptability in the real-life situations. Due to some popular as well as comparatively uncommon attack vectors, the security of cloud service has arose a big question in the success of the technology, resulting the need to measure the loss caused and also for adapting the appropriate countermeasures for those attacks.

In the present paper, a novel concept of Security Matrix has been proposed whose foundation is based on a mathematical model for computational easiness and technically based on security metrics of different types of attack vectors. The intention of the proposed matrix is to measure the impact of different types of attack vectors mathematically by using proper metrics and convert the weakness into strength by properly identifying the different types of threats and measuring the impact of the threats with proper and justified metrics in a definite manner.

Introduction

Cloud computing, a disruptive technology of the recent era, is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources having its intrinsic potentiality to enhance collaboration, agility, scaling, 24x7 availability with immense opportunity for cost reduction through optimized and efficient computing [1]. Its tremendous envision capability to cater components rapidly orchestrated, provisioned, implemented and decommissioned, scaling and on-demand utility-like model of allocation and consumption, is however, not free from some serious drawbacks due to its inherent security breach. Cloud computing is one of the most robust and popular technology adapted by industries showing the way to increase the capacity or add capabilities dynamically, without investing any new infrastructure. The agility, multi tenancy, virtualization and better performance of a cloud have made this technology enormously growing with the time. Although, cloud computing have been for decades, but of late, its inevitability in the industries ranging from medium to large and service to manufacturing could have been realized. That the recent IT industry could not survive without cloud is well sensed because of its wide adoptability and applicability not only to the hardware and software services over the internet, but also, for its embracement of multitude and multi-dimensional service capabilities ranging from mature sales force management to email and photo editing to the latest smart phone applications and the entire social networking phenomenon, to mention a few [2][3].

The only major apprehension of its unacceptability in the real-life applications is because of its weakness on privacy and security issues, which is obviously, a big concern for both for providers and users. With the improvement of technologies, the attackers or hackers are able to launch attack vectors over cloud services causing a headache to the service providers and users as well. Instead of so many clear benefits in the emerging cloud technology, the field is not picking up the pace as it should be because of the privacy and security issues lying intrinsically in the technology itself. Thus cloud security has become an evolving sub-domain under the arena of information security that consists of network security, data security and also the computer security as a whole. The major security threat for cloud computing are several attack vectors, which cause great impacts on cloud services, that includes viruses, e-mail attachments, Web pages, pop-up windows, instant messages, chat rooms and deception. In brief, due to some popular as well as comparatively uncommon attack vectors, the security of cloud service has arose a big question in the success of the technology, which is very essential to measure properly to ensure the loss caused and also for adapting the appropriate countermeasures for those attacks. Thus, the area of privacy and security in cloud environment has emerged as a powerful research area, which has been under consideration and strict observation by several cloud researchers [4] [5].

A good number of attack vectors and threats have been identified responsible for the decline of the widespread of the cloud computing in the IT and ITes industries and a major thrust research area has been evolved in the current decade, particularly, to device and formalize the appropriate security metrics for the measurement of the impact of the varied attack vectors. Threats are generally much easier to list than to describe, and much easier to describe than to measure. As a result, many organizations list threats, fewer describe them in useful terms and fewer measure them in meaningful ways. It has been observed that any system could be continuously monitored for several attack vectors and steps could be taken to control those attacks with appropriate measures. The domain of the problem is chosen in the cloud security area because of its novelty, importance, wide scope of research, applicability in the real-life industries and also the carry forward prospect in the relevant field for future research works [7] [8].

Architecture of the Cloud

From an architectural perspective, Figure 1, there is much confusion surrounding how cloud is both similar to and different from existing models of computing and how these similarities and differences impact the organizational, operational, and technological approaches to network and information security practices [2] [6].

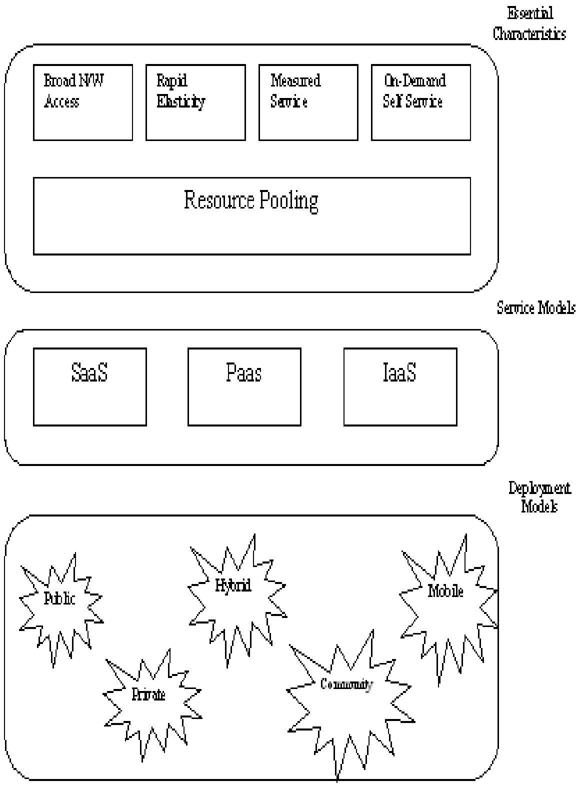

Figure 1. Cloud Architecture

A. Types of Clouds

There are basically three main types of clouds, viz., Public Cloud, Private Cloud and Hybrid Cloud. However, there are some special purpose clouds commercially used in this field, viz., Community Cloud and Mobile Cloud.

A.1 Public Cloud

Public cloud applications, storage, and other resources are made available to the general public by a service provider, using a free to all services or a pay per use model (Figure 2).

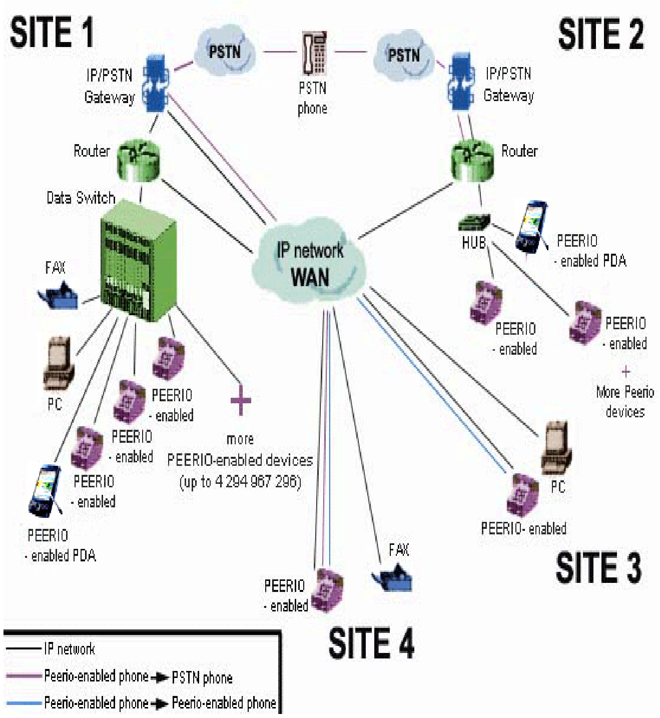

Figure 2. Public Cloud

A.2 Private Cloud

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally .It is also known as Internal Cloud or Corporate Cloud. Marketing media that uses the words "private cloud" is designed to appeal to an organization that needs or wants more control over their data than they can get by using a third-party hosted service. In Figure 3, a diagram for private cloud has been shown. Using Virtual Middleware (VM) or Virtual data center, the company can run their private cloud services.

Microsoft Azure, IBM, Sales force etc they run private cloud services.

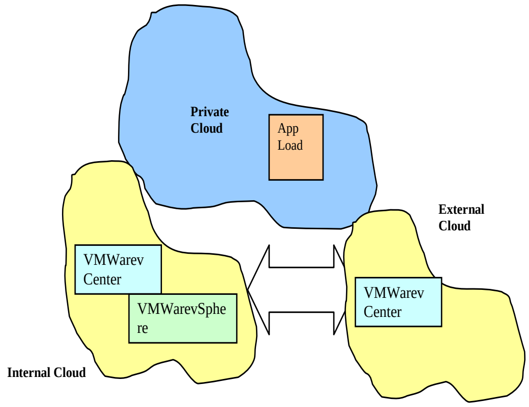

Figure 3. Private Cloud

A.3 Hybrid cloud

Organizations may host critical applications on private clouds and applications with comparatively less security concerns on the public cloud. In case of hybrid cloud computing, both private and public type of cloud computing is combined together. This is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models.

By utilizing "hybrid cloud" architecture, shown in Figure 4, companies and individuals are able to obtain degrees of fault tolerance combined with locally immediate usability without dependency on internet connectivity. Hybrid cloud architecture requires both on-premises resources and off-site server-based cloud infrastructure.

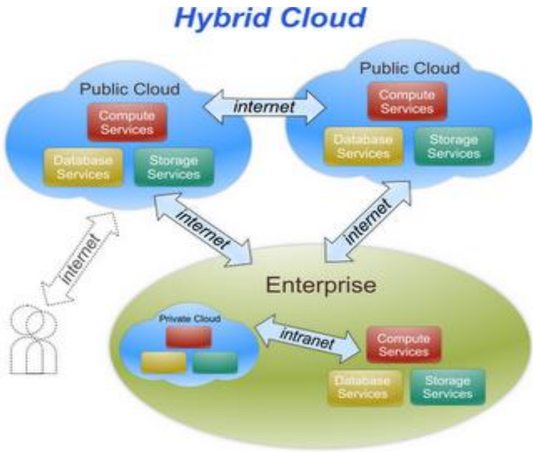

Figure 4. Hybrid Cloud

A.4 Community Cloud

A community cloud in computing is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized. Community cloud is a special type of service where a group of service providers united together and form a community depending on service type.

A.5 Mobile Cloud

Mobile cloud computing is the usage of cloud computing in combination with mobile devices. Cloud computing exists when tasks and data are kept on the Internet rather than on individual devices, providing on-demand access. In case of mobile cloud, Applications are run on a remote server and then sent to the user. Because of the advanced improvement in mobile browsers thanks to Apple and Google over the past couple of years, nearly every mobile should have a suitable browser. This means developers will have a much wider market and they can bypass the restrictions created by mobile operating systems. Mobile applications are a rapidly developing segment of the global mobile market.

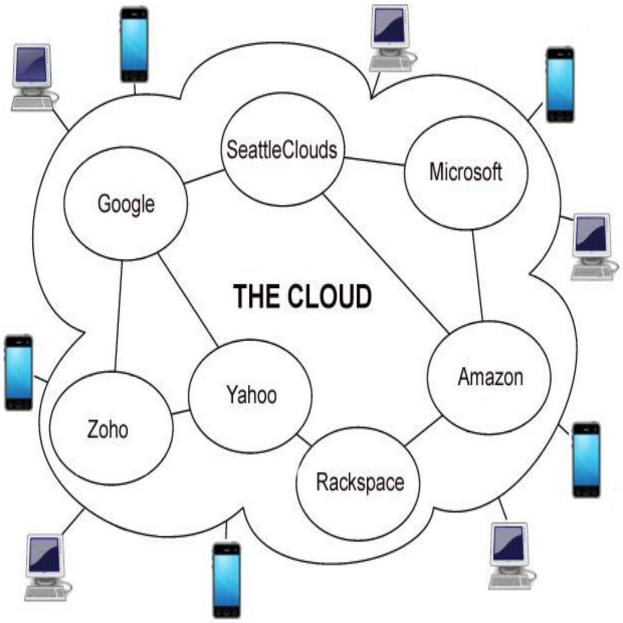

Figure 5. Mobile Cloud

Cloud Delivery Models

Cloud computing service providers deploy there services categorized mainly into these three following models [2][6]:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)

A.1 Infrastructure as a service (IaaS)

It is the delivery of computer infrastructure (typically a platform virtualization environment) as a service. Rather than purchasing servers, software, data center space or network equipment, clients instead buy these resources as a fully outsourced service. In this most basic cloud service model, cloud providers offer computers, as physical or more often as virtual machines, and other resources. The virtual machines are run as guests by a hyper visor, such as Xen or KVM. Examples of IaaS include Amazon Cloud Formation (and underlying services such as Amazon EC2), Rackspace Cloud, Terremark and Google Compute Engine.

A.2 Platform as a service (PaaS)

Platform as a service or PaaS provides the Application Framework-as-a-service layer upon which software applications can be securely and reliably built. Industry Analyst firm Forrester describes PaaS as an externally hosted service that provides a complete platform to create, run, and operate applications. It is another SaaS, where this kind of cloud computing providing development environment as a service. In the PaaS model, cloud providers deliver a computing platform typically including operating system, programming language execution environment, database, and web server. Some examples of PaaS are Amazon Elastic Beanstalk, Cloud Foundry, Heroku, Force.com, Engine Yard, Mendix, Google App Engine, Microsoft, Azure.

A.3 Software as a Service (SaaS)

This kind of cloud computing transfer programs to millions of users through browser. In the user's views, this can save some cost on servers and software. SAAS is commonly used in human resource management system and ERP (Enterprise Resource Planning). Google Apps and Zoho Office are also providing this kind of service.

Attack Vectors in Cloud

Attack vectors, one of the common and popular term in the world of cloud security, is the route or path through which the attacker gets entered into the system, mainly due to nefarious purposes. They take advantage of known weak spots to gain entry [7]. Many attack vectors take advantage of the human element in the *system*, because that's often the weakest link. Emails, the attachments carried by an email or the deception may be treated as an attack vector for malicious purposes. Hoax as an attack vector can damage the network also [8]. Even though they don't attack computers directly, ignorance and credulity is the attack vector here as it is being spread by multiple numbers of people. Web pages can be used as an attack vectors too. They can be rigged to do a number of things - virtually anything that a malicious email attachment can do. They take advantage of the power that modern browsers have to access several program languages -- Java, Javascript, ActiveX and Microsoft Word macros. Several Attack vectors have been discussed in the following few paragraphs followed by the threats or attacks over the cloud system [9] [10].

i) Denial of Service (DoS) attacks

This is a very common attack vector launched by an eavesdropper when hackers overflow a network server or web server with frequent request of services to damage the network, server could not legitimate clients' regular requests of the services. In cloud computing, hackers attack on the server by sending thousands of requests to the server that server is unable to respond to the regular clients in this way server will not work properly [11]. In the Figure 6, we have shown an image for the Denial of service attack where the master launches an attack through compromised zombie network.

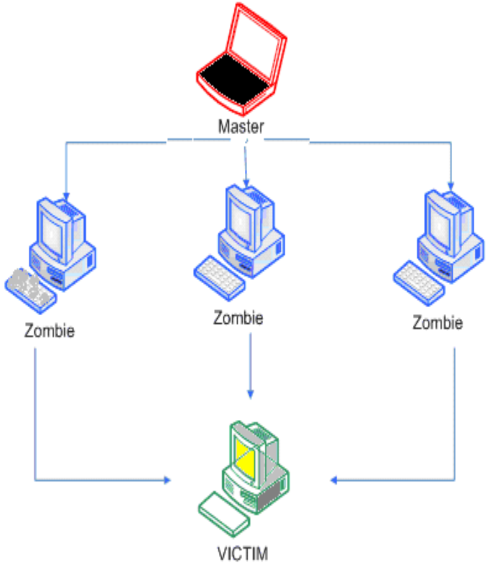

Figure 6. DoS Attack

ii) Cloud Malware Injection Attack

Usually when a customer opens an account in the cloud, the provider creates an image of the customer's VM in the image repository system of the cloud. In case of a malware-injection attack, the attacker takes an adversary attempts to inject malicious service or code, which appears as one of the valid instance services running in the cloud. If the attacker is successful, then the cloud service will suffer from eavesdropping [12]. The main idea of the Cloud Malware Injection attack is that an attacker uploads a manipulated copy of a victim's service instance so that some service requests to the victim service are processed within that malicious instance. In order to achieve this, the attacker has to gain control over the victim's data in the cloud system (e.g. using one of the attacks described above). This attack is the major representative of exploiting the service-to-cloud attack surface.

iii) Distributed Denial of Service Attack (DDOS Attack)

Distributed Denial of Service is a special type of DOS attack where multiple compromised systems are used, which are usually infected with a Trojan and used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS (Figure 6) attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack. This attack is now a days becoming a popular attack for cloud services [13].

In this attack, the eavesdropper being the master component, launches the attack on the victim, using a compromised network which is in turn divided into two separate layers . This attack is very vulnerable especially for shared environment like cloud, where sometimes even the service provider does not know from where the service has come to them and where the data has been stored.

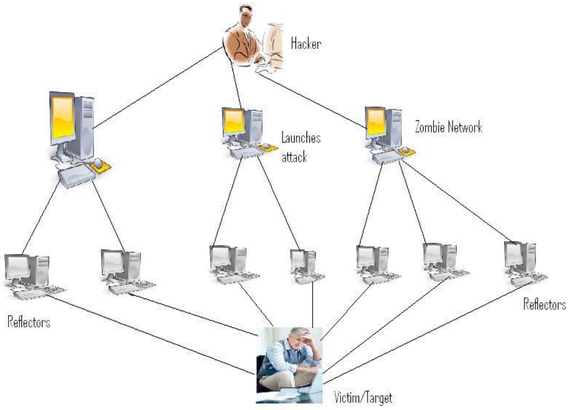

Figure 7. DDoS Attack

iv) Side Channel Attack

Within a piece of hardware that has multiple virtual machine resources are shared which can be used as a way to side channel data from one virtual machine to another. This type of attack is based on the shared resources between virtual machines within the same hardware. An attacker being successful in neighboring a target can then use various methods for intercepting data being sent and received from the other virtual machine. This form of security risk has been documented and there are many methods for preventing this type of attack.

v) Cross Site scripting Attack

Cross-site scripting attack (XSS) is a security exploit in which the attacker inserts malicious codes into a link that appears to be from a trustworthy source. When someone clicks on the link, the embedded programming is submitted as part of the client's Web request and can execute on the user's computer, typically allowing the attacker to steal information. So, instead of going to the original server address it will be directed to the malicious site. This attack has a great impact on cloud computing. SQL injection attack is a special type of such attack [14].

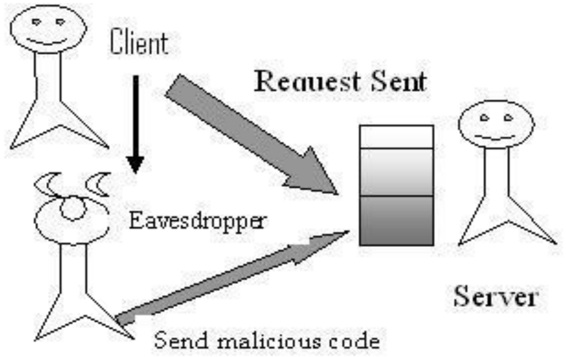

Figure 8. Cross Site scripting attack

vi) Man-in-the Middle attack

Man in the middle attack, shown in Figure 9, also known as fire brigade attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications, tamper data.

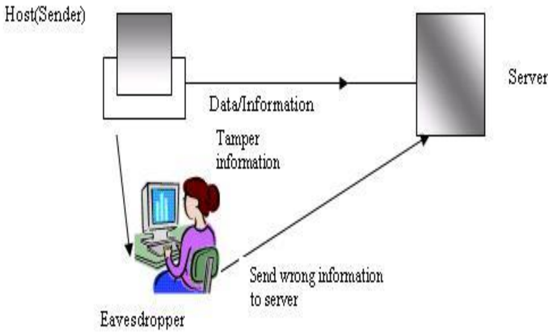

Figure 9. Man in the middle attack

vii) Wrapping attack

XML signature Element Wrapping is the fine renowned attack for web service. This attack is done by duplication of the user account and password in the log-in phase so that the SOAP (Simple Object Access Protocol) messages that are exchanged during the setup phase between the Web browser and server are affected by the attackers. Attacker targets the component by operating the SOAP messages and putting anything that attacker likes, as shown in Figure 10.

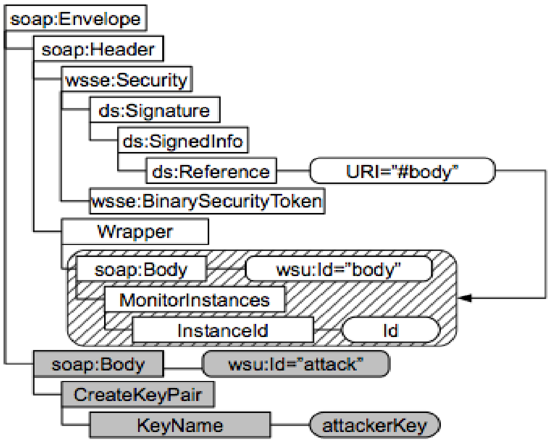

Figure 10. Wrapping Attack

viii) Flooding attack

In this attack, the attacker launches the attack openly. The most significant feature of cloud system is to make available of vigorously scalable resources. Cloud system repeatedly increase its size when there is further requests from clients, cloud system initialize new service request in order to maintain client requirements. Flooding attack is basically distributing a great amount of meaningless requests to a certain services which flood the server.

Once the attacker throw a great amount of requests, by providing more recourses cloud system will attempt to work against the requests, ultimately system consume all recourses and not capable to supply service to normal requests from user. Then attacker attacks the service server. DOS attacks cost extra fees to the consumer for usage of recourses. In an unexpected situation the owner of the service has to compensate additional money. Counter measure for this attack is it's not easy to stop Dos Attacks.

ix) Network Sniffing Attack

Network sniffing attack is more critical issue of network security in which un-encrypted data are hacked through network for example an attacker can hack passwords that are not properly encrypted during communication. If the communication parties not used encryption techniques for data security then attacker can capture the data during transmission as a third party. Counter measure for this attack is parties should used encryption methods for securing there data.

x) Problem of Cheap data and data analysis

Access of data in cloud is cheap. But along with this it brings some problems. Because of the cloud, attackers potentially have massive, centralized databases available for analysis and also the raw computing power to mine these databases. Synchronizing data is a problem. An example of indirect data-mining that might be performed by a cloud provider is to note transactional and relationship information. But this problem can be solved by proper tracking of IP

xi) Port Scanning

There are some issues faced by the cloud providers regarding port scanning that could be used by an attacker as Port 80(HTTP) is always open that is used for providing the web services to the user. Other ports such as 21(FTP) etc are not opened all the time it will open when needed therefore ports should be secured by encrypted until and unless the server software is configured properly. The approaches has been taken to dissolve this attack is that firewall is used to secure the data from port attacks.

xii) Accountability Check problem

The payment method of cloud system is “No use No bill”. When a customer launches an instance, the duration of the instance, the amount of data transfer in the network and the number of CPU cycles per user are all recorded. Based on this recorded information, the customer is charged. But with the accountability check problem, an attacker has engaged the cloud with a malicious service or runs malicious codes, consuming a lot of computational power and storage from the cloud server and as a result, the legitimate account holder is charged for this kind of computation which he or she have not taken in actual. Hence, a dispute arises and business reputations are hampered [15][16].

Security Matrix: Proposed Work

As the security has become a vital issue for the widespread of cloud computing both from the viewpoint of providers and users as well, in the present work, a novel concept of Security Matrix (SM) has been proposed, which is mathematically based on a multidimensional matrix for computational easiness and technically based on cloud security metrics. The primary objective of the proposed work is to first identify the different types of possible attack vectors including traditional as well as specialized attacks, which could be possible by continuously monitoring the networks, and then to measure the impact of different types of attack vectors with proper and justified metrics forming logical distinctive security matrices. The proposed model could be used not only for cloud security but also to measure the impacts of any type of attacks or threats in traditional networks. The strategic objective is to convert the weakness into strength by properly identifying the different types of threats and measuring the impact of the threats in a definite manner [17-21].

Here, investigating all possible circumstances, we have considered five different types of security matrices, as given below, to measure the impacts of the threats,

1. Asset Matrix(AM)
2. Hazard Matrix(HM)
3. Vulnerability Matrix(VM)
4. Threat Matrix (TM)
5. Capacity Matrix(CM)

In financial accounting, assets are economic resources. Anything tangible/ intangible that is capable of being owned or controlled to produce value and that is held to have positive economic value is considered an asset. In case of cloud computing, as it is on demand service, the asset loss has a great impact and in our proposed model asset is thinking of being measured in terms of Return on Total Asset (ROTA), TA index measurable in terms of finance management.

Asset Loss Matrix (ALM) =

$$\begin{pmatrix} \text{Lost TA Index} & \text{Intangible Asset Loss} \\ \text{NROSI Index} & \text{Market Disruption Rate} \end{pmatrix} \begin{pmatrix} wf1 & wf2 \\ wf3 & wf4 \end{pmatrix}$$

Here, TA=Tangible Asset.
Lost TA Index=ROTA of Company / Loss of TA of company due to an attack.

Where, ROTA=Return on Total Tangible Asset. This is a ratio that measures 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

The company needs not to provide their confidential data for measuring this value. If this Lost TA index having a high value, the company can provide the value “2” for a high range of lost TA index, for medium range it will be 1 and for a negligible range of Lost TA index 0 has been considered to put.

Intangible asset loss parameter is having a Boolean value for its presence or absence- having value either 1 for presence or 0 for absence.

Return on security investment (ROSI) is again a measurable quantity. This can be measured as
Non-ROSI (NROSI) Index=1/ROSI

Return on security investment (ROSI) =
(Risk Exposure * %of Risk mitigated – Solution Cost)/ Solution Cost

If this rate is low the attack is treated as more harmful, value should be high for this.

With the **market disruption rate** of an attack, the loss due an attack can be measured. If this value gets high, it should be assumed as 2, where as value having a low market disruption rate may be treated as 0.This assumption should made on the basis of the current industry standard and study.

A **hazard** is a situation that poses a level of threat to life, health, property, or environment in real life scenario. We can categorize hazard into three different types – Dormant, Armed and Active. Most hazards are dormant or potential, with only a theoretical risk of harm; however, once a hazard becomes "active", it can create an emergency situation [22].

In our proposed hazard matrix, the parameters are measured using different real-life aspects like health hazard, technological hazard or environmental hazard that may have been caused by an attack vector and in which respect it is measurable.

Hazard Matrix (HM) =

$$\begin{pmatrix} \text{Technological Hazard} & \text{Operational Hazard} \\ \text{Environmental Hazard} & \text{Physical Security Hazard} \end{pmatrix} \begin{pmatrix} wf1 & wf2 \\ wf3 & wf4 \end{pmatrix}$$

Technological Hazard can be measured against some technological problem lists like server problem facing due to an attack
Operational Hazard parameter shows the problems faced while operating a cloud system.

Environmental Hazard is a parameter which can be indirectly measured by measuring the green cost of cloud. For example, if due to an attack the power consumption rate of a cloud system increases, and it is possible to measure this, then this leads to the environment hazard as then the cloud system will not be considered as energy efficient.

Physical Security Hazard is a parameter which shows the problem faced by physical security of a system, consisting a Boolean value from 2 to 0.Suppose, for an inside malicious user, due to the wrapping attack or side channel attack, the system security being endangered, causing problem, then it may be assumed as having the value 1, as physical security is being hampered.

Threat is measurable by its degree of criticalness or by threat event frequency, for which the threat matrix is being proposed considering several relevant parameters.

Threat matrix(TM) =

$$\begin{pmatrix} \text{Threat Responsiveness} & \text{Ease of Recovery} \\ \text{Deployment Model} & \text{Threat Event Frequency} \end{pmatrix} \begin{pmatrix} wf1 & wf2 \\ wf3 & wf4 \end{pmatrix}$$

Threat responsiveness of a system shows how fast a system could response to a threat. If it takes a low time to response to a new threat, the value gets high and may be assumed as 2, nominal value is 1.

Ease of recovery of a threat proves the criticalness of the threat somewhat. As less time it takes, as easier to handle. The value having 2 requires more effort in recovery, where as the value 0 proves that it is much easier to recover the threat.

Vulnerability is the probability that an asset will be unable to resist the actions of a threat agent. Vulnerability exists when there is a difference between the force being applied by the threat agent, and an object's ability to resist that force (According to Open Group's risk taxonomy).It is a prominent factor of risk. ISO 27005 defines risk as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization" [23].

In the proposed vulnerability matrix (VM), the probability for a system of being vulnerable is trying to be measured with some real-life observations like no of suspected compromised network present, or how much the system is threat-responsive.

Vulnerability Matrix (VM) =

$$\begin{pmatrix} \text{Prevalence of attack} & \text{System Responsiveness} \\ \text{Compromised N/w level} & \text{SLA Response PE} \end{pmatrix} \begin{pmatrix} wf1 & wf2 \\ wf3 & wf4 \end{pmatrix}$$

The parameter **Prevalence of attack** measures the frequency or occurrences of attack on a system. This is again assumed as having four different values – 3,2,1,0. If the frequency is more than 50 then it can be assumed as 3…in between 49-20, it is 2. The frequency having less than 10 attacks on a system will be treated with value 0.

Presence of **Suspected compromised networks** or more popularly known as Botnets, can make a system vulnerable. So the number of Botnet is important while considering system vulnerability. In this parameter, there is an indirect measure of the number of suspected network. If this level is high, we can limit the number or range as 2.The suspected network having value less than or equal to two networks or with no such network presence, will be considered with value 0.

The **SLA response Error probability** is a parameter which measure error in the response rate of Service level agreements. A cloud system should response the service level agreements in time, unless it will be a vulnerable one. If this value gets high, it will be with a higher probability. Here, for the ease of our calculation, we have also assumed those values into three different values- 2, 1 and 0.The value with a higher SLA response error rate is considered as having a value 2.0 is the lowest range.

Capacity, unlike the other terms, is itself a positive term which measures the system strength and effectiveness. In our proposal, the **capacity matrix** hence reflects the positiveness of a cloud system.

Capacity Matrix (CM) =

$$\begin{pmatrix} \text{Fault Tolerance} & \text{Control Strength} \\ \text{Degree of multitenancy} & \text{Virtualization Potential} \end{pmatrix} \begin{pmatrix} wf1 & wf2 \\ wf3 & wf4 \end{pmatrix}$$

Control strength of a system is a valuable parameter and it can be determine by comparing how much perfect a system be even after being attacked. We can measure the control strength by the following approach. This term is much more applicable in mechanical engineering. But for cloud system also, this is a measurable parameter. Again for the ease of our calculation, we have assumed three differen high control strength. The values are –

$$\begin{pmatrix} wf1 & wf2 \\ wf3 & wf4 \end{pmatrix}$$

Control strength = (No. of checkpoi to prevent an attack/ No. of them are successful) x 100

The **Degree of multi tenancy** of a system gives a clear picture of it's capacity. Much higher the value it contains, much stable the system is. This parameter is as-

sumed the value with 3,2,1,0 as well. A system able to serve more than 50 tenants without a problem, having value 3. The lowest value 0 will be assumed in case of a system containing less than or equals to 5 tenants or in case of a private internal cloud system.
The term **Virtualization Potential** is an important parameter for measuring the system strength.

The proposed new resultant matrix, viz., Risk Matrix, hence will be as follow:

Risk-Matrix(RM)= ± {{ [ALM] * [VM] * [TM] * [HM] } – [CM]}

With sufficient data and observation result for each parameter, our proposed model may measure the impact of an vector over a system, by measuring the **Risk-factor** (Rf), which in turn may be measured by determinant of the matrix [19].

Conclusions and Future Works

The privacy and security area in cloud computing leaves an ample scope for the cloud researchers and developers towards the design and development of proper measurement tools to quantitatively measure the impact of different types of attack vectors so that justified evaluation of threats could be done and proactively appropriate countermeasures could be taken. It is observed that all threats are not of same value, i.e., not equally harmful. Where, some are critically dangerous, some could be ignored even, and thus the requirement of identification, categorization and proper measurement of the harmfulness of different types of threats or attack vectors have become essential primarily for the cloud providers using proper metrics and tools to increase the province of their business by spreading the domain of the concerned technology.

In the present proposal, a novel concept of Security Matrix (SM) has been brought into light, which fundamentally lays its foundation on very simple mathematical model of multidimensional matrices but technologically based on security metrics of attack vectors in the area of cloud security. Currently, five different types of Security Matrix or SM have been proposed as well as their parameters have been formalized to measure the impact quantitatively, which, in future, could be extended, if found coherent and apposite to real-life scenario followed by requisite survey and investigations. These five matrices have been constructed with varied dimensions keeping the content as simple and practicable as possible to draw quantitative inference of different types of attack vectors by calculating weights of individual parameters and then computing ranks of different matrices. Different types of parameters and factors are also in consideration in each matrix and appropriate weights have to be attached to make the measurements quantitative rather than qualitative. An extensive survey among heterogeneous IT and ITes organizations have been done to identify and attach weights and thresholds to each individual parameter of different matrices of the SM to construct the total SM as proposed in this paper.

A lots of research scope has been identified in the specified field and our future goal is to formalize the concept of Security Matrix in more concrete way by incorporating more meaningful and justified real-life parameters and to develop a decision making tool using which providers and/or users could be able to measure the impact of different types of threats very easily as well as effectiveness of adapting a particular cloud system.

References

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

[2] Resse, Mather, “Cloud Application Architecture: Building Applications and Infrastructure in the Cloud”, SPD O’Reilly publication, 2009

[3] http://en.wikipedia.org/wiki/Cloud_computing.

[4] Stevenson, “Cloud Security and Privacy”, SPD O’Reilly publication, 2010

[5] Mohit Mathur, KLSI, “Cloud computing Black Book”, Wiley Publication, 2012

[6] Wilder, “Cloud Architecture Patterns”, SPD O’Reilly publication, 2012

[7] 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.

[8] http://searchsecurity.techtarget.com/definition/attack-vector.

[9] B.Meena- Dept. of Information Technology, ANITS, Visakhapatnam, AP, Krishnaveer Abhishek Challa , Dept. of Electrical Engineering, Blekinge Institute of Technology, Sweden, ” Cloud Computing Security Issues with Possible Solutions”, IJCST Vol. 3, Issue 1, Jan. - March 2012.

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

[11] Sara Qaisar, Kausar Fiaz Khawaja (Corresponding Author), “Cloud Computing: Network/Security Threats And Countermeasures” published on Interdisciplinary Journal Of Contemporary Research In Business on January 2012, VOL 3, NO 9.

[12] Timothy K. Buennemeyer, “A Strategic Approach to Network Defense: Framing the Cloud”, Autumn 2011

[13] Muhammad Imran Tariq, Department of Computer Science and Information Technology, University of Lahore, “Towards Information Security”

[14] Mario Heiderich, Marcus Niemietz, Felix Schuster, Thorsten Holz, Jörg Schwenk, “Scriptless Attacks – Stealing the Pie Without Touching the Sill”

[15] Nelson Gonzalez, Charles Miers, Fernando Red Igolo, Marcos Simplıcio, Tereza Carvalho, Mats N¨aslund and Makan Pourzandi, “A quantitative analysis of current security concerns and solutions for cloud computing”, Journal of Cloud Computing, Springer Open Journal,2012

[16] “Security guidance for critical areas of focus in cloud computing v3.0”, Cloud Security Alliances, 2

[17] Nielsen, Fran. “Approaches to Security Metrics.” NIST and CSSPAB Workshop, Washington, D.C., 13-14 June 2000:7. URL: http://csrc.nist.gov /csspab/june13-15/metrics_report.pdf (10 July 2001)

[18] Nia Ramadianti Putri, Medard Charles Mganga, “Enhancing Information Security in Cloud Computing Services using SLA Based Metrics” published on Master Thesis Computer Science, Thesis no: MCS-2011-03, January 2011

[19] http://www.darkreading.com/security-monitoring /167901086 /security/perimeter security/ 232600679/ five-tactical-security-metrics-to- watch.html

[20] “Metrics Framework for Cloud Computing” published on International Journal of Cloud Computing and Services Science, Vol.1, No.4, October 2012

[21] SANS Institute InfoSec Reading Room, “A Guide to Security Metrics”, published from SANS Institute in 2007

[22] http://en.wikipedia.org/wiki/Hazard

[23] http://www.infoq.com/resource/articles/ieee-cloud-computing-vulnerabilities.htm

Biographies

SANTANU KUMAR SEN received the B.E. degree in Computer Science & Engineering from Regional Engineering College, Silchar, Assam in 1994, the PhD(Engg.) degree in Computer Science & Engineering from Jadavpur University in 2008, the MBA degree in Information Systems from Sikkim Manipal University, Sikkim in 2011 and the M.Tech degree in Computer Science & Engineering from CMJ University, Shillong, in 2013 respectively. He is a Fellow of IET(UK), IE(I), IETE(I) and Sr. Member of IEEE (USA), CSI(I) and life members of ISTE. He is currently working as Professor and Head in the Department of Computer Science & Engineering in Gurunanak Institute of Technology. His teaching and research areas include Mobile Ad Hoc Networks, Computer Networks, Sensor Networks and Cloud Computing.

SHARMISTHA DEY received the B.S Degree from University of Calcutta in 2004, the MCA degree from West Bengal University of Technology in 2007 and M.Tech degree in Computer Science and Applications in 2013 from University of Calcutta. She also possesses Post Graduate Diploma in Mass Communication, Public Relations and Journalism. She is an Associate Member of CSI(I). She is currently working as Assistant Professor under the Department of Computer Application in Gurunanak Institute of Technology. Her teaching and research areas include Cloud Computing and Computer Networks and Mobile Communication. Ms. Dey may be reached at