An Inside Attack Assessment Model For Infrastructure As A Service In Cloud Trust

Jasdeep Singh, Manoj Kumar, Sukhwinder Singh Sran

Abstract: In these days Cloud computing is providing us a suitable choice of computing and storage of the resources mainly for the business in which user "pay per usage". But most of the organizations are not using the cloud due to the lack of the trust on the service provider. Nowadays data breaches in cloud services are also increasing year-by-year by the hackers which are trying to compromise the security of the cloud. In this work, we have performed a depth analysis of cloud trust models for the existing functional and non-functional aspects to accurately evaluate the trust of the cloud provider and the theory of assessment of the security level of insider threats. We describe the modelling methodology which captures several aspects of insider threats and shows threat assessment methodology to reveal the possible attack strategies of an insider.

Index Terms: Cloud Computing, Assessment Models, Security, Threats, Attacks.

1. INTRODUCTION

Cloud is a collection of Data center, Virtual machines which are paid as well as free services and resources provided by some company like Amazon, Google cloud platform, Rackspace, Microsoft Azure, etc. Cloud computing can provide Hardware, Software and Memory space over the internet. Cloud environment provides offerings over Public, Hybrid Networks, Local Area Network (LAN) and Wide Area Network (WAN). Packages like electronic mail, social networking, Consumer Relationship Management (CRM), YouTube make the use of cloud computing.

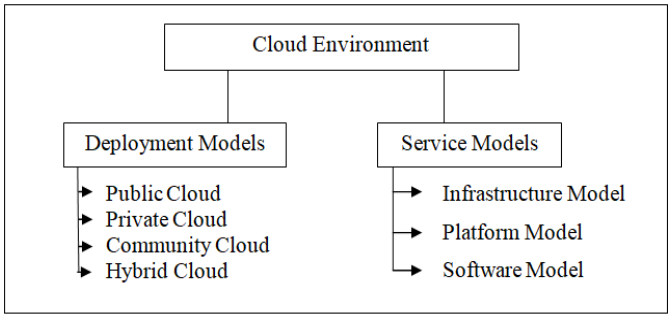


Fig1. *Basic Concepts of Cloud Computing*

we use different search engines and there cloud servers for storing our search results (Google, yahoo, Bing); use of email services for exchange of data and information to someone (Google, Yahoo and etc); use of the social networking websites for messaging to friend and stay connected with them (Face book, MySpace and Twitter); for the storage purpose of music, image, videos and documents (Drop box, iCloud, etc); in cloud computing also the facility of online backup of the system or the data which automatically backup the file over the internet(Jungle Disk, IDrive, Elephant Drive, etc). Various organizations are also using Cloud for their business purposes. These organizations rent the servers, virtual machine and the other resources from the cloud services provider and pay the services provider as per usage of the resources. It saves maintenance and the operational cost of the resources. For example: a social news website rents Amazon elastic compute cloud (EC2) for their digital bulletin board services [1] There is no question on the resources and the less cost of the cloud services changed our lives; but there are still some security issues in cloud computing that scares everyone to use it, which are happening in daily life, like cyber crimes. Hackers use the lots of techniques to compromise the access of the cloud server without using the legal authentication. It is a challenge to provide the competent security to the cloud services so user can use without any risk.

Three main objectives are discussed based on the cloud services [2]

- Confidentiality: it refers to the prevention the unauthorized access of data and make sure that data is accessible only by authorized user.
- Integrity: It assures that data is not changed neither when it is stored nor while it is trans formed over the network
- Availability: It assures that services and the data will be available when it needed.

These security objectives need use of security mechanism and services to be implemented. So, we will be able to identify the process, a device aimed to detect, prevent and recover the attack. Several security techniques are used like encryption, cryptography and hash function to ensure the security of cloud Services. Because once the exact location of the data is captured by the hackers, they will use the information and the data for wrong purposes. They will steal the private information to misuse and share it with other users. In leakage accident, Epsilon leaked million of names and email address from the customer database. Stratford's 75,000 credit card numbers and 860,000 user names and passwords were stolen [3].

1.1SERVICE MODEL:

Cloud computing includes providing of the services (storage, application, and server) to the user through various service providers. The user can access the cloud assets by the internet. Cloud services provider grantee the merit of services. In cloud computing, there are three layers in cloud service model: platform layer, application layer, system layer. The first layer or bottom layer is the system layer which includes the

- *Jasdeep Singh is currently pursuing M.Tech in Computer Engg. from YCOE, Punjabi University Guru Kashi Campus, Talwandi Sabo, India, E-mail: jasdeep1007@gmail.com*
- *Manoj Kumar, Assistant Professor, YCOE, Punjabi University Guru Kashi Campus, Talwandi Sabo, India*
- *Sukhwinder Singh Sran,, Assistant Professor, YCOE, Punjabi University Guru Kashi Campus, Talwandi Sabo, India*

memory, network devices, storage and the computational assets for example infrastructure of servers. System layer is also known as infrastructure as a service. Computational assets are made available to the user as per demand. Infrastructures as a service also provide the virtual machines by which user can create a complex infrastructure. It reduces the cost of buying the physical resources and also reduces the load of the network administration because IT professional is not needed for the monitoring of the physical network. For instance, Amazon's EC2 [1] that provide the virtual computing with the network interface, by using this interface user can use virtual machines over Linux, Window, and Solaris and run their own applications.

TABLE 1 *Cloud Service Provider on Cloud Service Models*

Cloud Service Models	Cloud Service Provider
SaaS	Antenna Software, Cloud9 Analytics, Google Apps, Microsoft 365, Rackspace and IBM.
PaaS	Google Apps, NetSuite, WorkXpress and Microsoft Azure.
IaaS	Amazon Elastic Compute Cloud, Rackspace, Bluelock and Open stack.

The middle layer is platform layer which is specially designed for the user to develop their specific application. This layer is also known as the platform as a service. This model provides the tools and the libraries for the development of the applications and allows the user to control over the application development and configuration settings. By using the PaaS user does not need to buy software development tool, hence it also reduces the development cost of application. Google apps are an example of PaaS it is a package of Google tools. That provides Google search engine, Gmail, Google Groups, Google Talk and Google Docs. It gives the user to customize their tools over his domain. The top layer is the application layer, it is also known as software as a service (SaaS). Application layer provide the services to the rent running applications over the cloud instead of purchasing. It reduces the cost of the application so; SaaS is popular in organizations. For example, providing online support system it processes thousands of tickets more efficiently of their daily customer [1]. Table 1 is the example of cloud service provider on three cloud service models. In cloud computing, these are three main services models out of five. In this mainly the concentrate on the bottom layer which is IaaS. It is the layer which provides the access control of the virtual infrastructure like a virtual machine. Cloud IaaS have changed everything in developer's way to deploy their applications. Before that developers spend their lots of time for own data centers, managing and hosting companies or services and then they hire operational staff to perform the operations. Now just only go to one of the IaaS providers, get a virtual server within a minute [4] and pays as per usage. IaaS is completely distant from the hardware and provides users to use infrastructure without disturbing anything the basic difficulties. IaaS gives only fundamental security Such as perimeter, firewall, load balancing, etc. and application running in the cloud will need an advanced level of security granted at the host [4].

1.2Threats to Cloud Computing

In this section we consider threats related to cloud service in security architecture. Here are some possible threats which are related to cloud and IaaS based on review of papers and knowledge [11].

- Change in Business Model: Cloud computing changes the technology and way of IT services. Services are provided by external service providers but business needs to assess the risks related with the failure of manage over the infrastructure. This is the higher threats which get in the way of usage of cloud computing services.
- Insecure Interface and APIs: Service provider frequently provides the set of APIs to the user to design an interface to communicates with the cloud service. These interfaces add a level on the top of the structure that increases the complexity of the cloud. It allows the vulnerabilities to move to the cloud environment. Offensive use of those interfaces poses threats like clear text authentication, improper authorization and broadcast of content. Such kind of threats may affect the IaaS, Saas and Paas.
- Malicious Insider: Most of the organization hides their procedures in the access of the employees and their using policies for the employees. Then how a user can get the access of confidential data and policies. It always happens due to lack of clearness in cloud provider procedure and process. Mostly Inside threats use the bypass through the firewall so the detection system thinks that it is a legal user or activity. In this condition insider can harm the cloud service providing. For example, insider can get private data and can access the control over the services without any detection risk. These types of threats also related to IaaS, SaaS and PaaS.
- Shared technology issues: In shared technology architecture, virtualization is used to provide on-demand shared services and same application is used by different users to get access the virtual machine. There vulnerabilities allow a malicious to gain the control and access another user's virtual machine. IaaS services are used over mutual assets, which might not be intended to afford strong isolation.
- Data Loss and Leakage: Data can be negotiated in different types. This might contain data negotiation, removal, or change. Because of the dynamic and divided nature of the Cloud, these threats can provide a key issue leading to information theft. Examples of these risks are lack of verification, weak encryption, approval and review control procedures. This threat can applicable to IaaS, SaaS, and PaaS.
- Identity theft: Identity theft is a type of scam in which someone makes believe to be someone else, to use assets or get credit and other profit. The casualty (of identity theft) can experience poor cost and losses and supposed responsible for the executor actions. Significant security threats contain weak password recovery techniques, key loggers and etc.

2 LITERATURE REVIEW

Chou et al. [1] Clouds provide a powerful computing platform that enables individuals and organizations to perform variety levels of tasks such as: use of online storage space, adoption of business applications, development of customized computer software, and creation of a "realistic" network environment. In previous years, the number of people using cloud services has dramatically increased and lots of data has been stored in cloud computing environments. In the meantime, data breaches to cloud services are also increasing every year due to hackers who are always trying to exploit the security vulnerabilities of the architecture of cloud. In this paper, three cloud service models were compared; cloud security risks and threats were investigated based on the nature of the cloud service models. Real world cloud attacks were included to demonstrate the techniques that hackers used against cloud computing systems. In addition, countermeasures to cloud security breaches are presented. Mohammed et al. [2] in this paper researcher aimed to provide information about present threats and attacks in cloud computing. There are most effective threats and attacks in cloud computing such as: data loss, data breach, hijacking, service traffic, etc. With the increase in using cloud computing by many users and organizations security issues also arise. This paper also considers about cloud computing objectives, its service models and suggest mitigations techniques which can help to improve cloud security or reduce the risk of threat in cloud. Ramkumar et al. [4] this paper discussed about insider attacks which can cause highly loss to any user or organizations. Inside threats are like sleeping cells which we don't know but they are working under the nose. Inside attack or threat is attributed as legitimate users which can maliciously influence their system rights and familiarity to computational environment for compromising valuable data/ information or for inflict damage. Due to lack of techniques and system tools security analyst sometimes do not notice the threat so that consider attack as inevitable. This paper also presents some theory of inside attack assessment and describe a modelling methodology which can capture different aspects of inside attack or threat and then, show threat assessment methodologies to disclose promising attack strategies of inside attack. Shital et al. [5] this paper introduces the base of security analysis of cloud environment in form of threats, impacts and vulnerabilities. In this analysis researcher defined top three threats in cloud computing with recommendation for practitioners. These top three threats are: conflicts between customer procedures and cloud provider procedures, physical threat, malicious insider and also gives countermeasures for this. The end of this analysis is that most serious threats to cloud computing are non- technical and can be solved by managing processes rather than technical countermeasures.

TABLE 2 *Top three issues and their countermeasures [5]*

Issue	Countermeasure
Conflicts between customer procedures and cloud provider procedures	Exhaustively research and staffed service level agreement contracts
Physical threat	Standard FISMA Physical security procedures
Malicious insider	Standard FISMA Personal security procedures

Makhdoom et al. [6] this paper introduces to virtualization of techniques that combines or divide computing resources to provide one or more execution environment using a technique which is software and hardware division, overall or partial machine simulation and mirroring. Virtualization is software which gives access to one physical server to compile a number of separate computing environments. It is a most important technique in cloud computing. Cloud service providers have a number of data hubs which are packed with servers to exchange cloud services of the servers but they are not capable to give a separate server to every user. So, they split the data on the server, enabling every client to use with different "virtual" case of the similar software. This paper also shares feature, limit, advantage and disadvantage of cloud computing and virtualization. Main focus of this paper is to compare virtualization and cloud computing. Seccombe et al. [7] this paper introduces with a set of most excellent security practices. Cloud security alliance has place together for operating or governing the cloud(data security and information management, cloud architecture, portability and interoperability, application security, data center operations, encryption and key management, access and identity management, security as a service and virtualization. It describes that IaaS platform can be encrypted by different techniques, depending on our data such as: Platform storage encryption, object and file storage. It also considered that some vulnerability assessments also needed in cloud computing for both contractual and architectural limitations.

3 PROBLEM FORMULATION

Trust Assessment is getting key priority with the growth of cloud service providers that take and store user data in their Data warehouses. Trust assessment provides the user with a level of trust in the provider as enterprise and user data security is a key parameter. Various trust assessment models have been developed, each having a different way to define trust etc. In this review, we have looked upon at various trust assessment models namelyIn the papers, it is demonstrated that Cloud-Trust is often accustomed assess the protection standing of IaaS CCSs and IaaS CSP service offerings and the way it is accustomed reason possibilities of Advanced Persistent Threats (APT) infiltration and possibilities of APT detection. There is some problem which we have nailed down after analyzing the work.

- The scope of presented work is limited to IaaS CCSs and CSPs.
- It does not cover inside attacks like attacks by authorized user

It does not detect tunneling paths of multiple servers which are also used for inside attacks

4 PROPOSED RESEARCH METHODOLOGY

This work is to actualize the Assessment of inside attacks in the cloud using Mat lab the implementation is performed. For technical computing, Matlab is a high-performance language. It combines computation, visualization, and programming in an easy-to-use environment where problems along with solutions are expressed in familiar mathematical notation. For high-productivity development research and analysis such as computations, algorithm development, Math, data visualization and analysis, scientific graphics, data acquisition, modeling, engineering graphics, simulation, and muchmore. Matlab is considered as one of the best tools. Matlab is a user-friendly system whose basic data element is an array that does not require dimensioning. This reason helps many technical computing problems to get solved, especially problems related with matrix and vector formulations. In threat assessment system, the following system is used to design the model for detection of a malicious insider. In the threat assessment the following steps are followed:

Step 1: Generating a Cloud Architecture
The cloud architecture is generated by generating a number of servers (VMs), Firewalls and Databases.
Step 2: Generate Random Access Requests
The model is generated for generating random access requests. Then based on binomial distribution some of the random requests are marked malicious.
Step 3: Mark each Malicious Request as Successful or Unsuccessful
Use binomial distribution to mark each malicious request as successful or unsuccessful. This will be used to compute the probability.
Step 4: Compute Combined Probability P (A|B)
Since the previous level is successfully hacked, use the probability of successful attack at next level using joint probability P (A|B).
Step 5: Similar to the forward probability, compute the reverse probability
Step 6: Perform the steps 'N' times to get the average probabilities in forward and reverse directions.
Step 7: Compute Average Security Measure of Probabilities

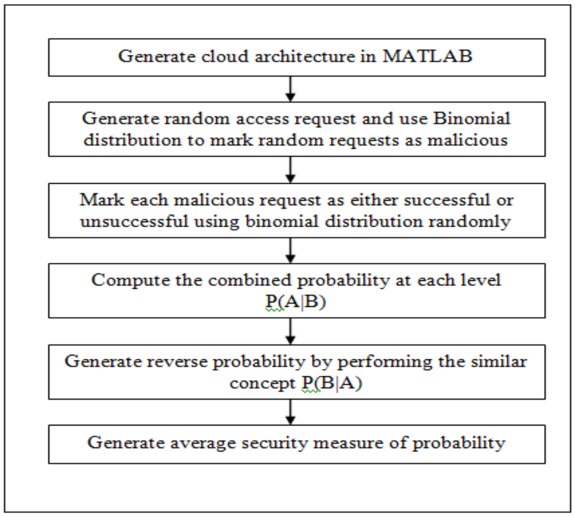

Generate cloud architecture in MATLAB
Generate random access request and use Binomial distribution to mark random requests as malicious
Mark each malicious request as either successful or unsuccessful using binomial distribution randomly
Compute the combined probability at each level P(A|B)
Generate reverse probability by performing the similar concept P(B|A)
Generate average security measure of probability

Fig 2: *Data Flow for the Proposed Algorithm*

5 SIMULATION AND EXPERIMENTAL RESULT

In this section results of proposed method is presented and discussed. The proposed method is implemented in Matlab. In the proposed method, the cloud architecture is generated by generating a number of servers (VMs), Firewalls and Databases. The system is generated by generating random access requests. Then based on binomial distribution some of the random requests are marked malicious. Use binomial distribution to mark each malicious request as successful or unsuccessful. This will be used to compute the probability. Since the previous level is successfully hacked, use the probability of successful attack at next level using joint probability P (A|B).

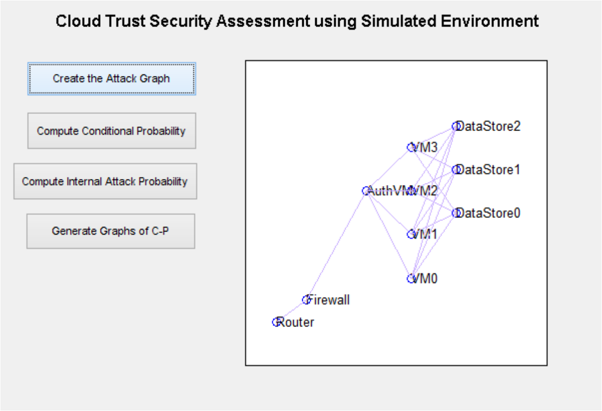
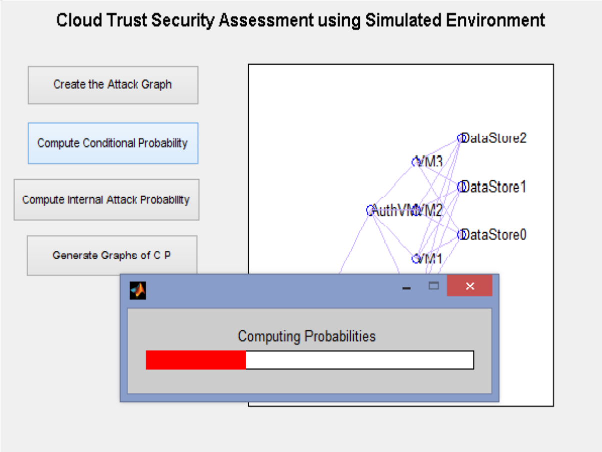

Cloud Trust Security Assessment using Simulated Environment
Create the Attack Graph
Compute Conditional Probability
Compute Internal Attack Probability
Generate Graphs of C-P
DataStore2
VM3
DataStore1
AuthVM
VM2
DataStore0
VM1
VM0
Firewall
Router

Fig 3: *The Image Showing the Attack Graph.*

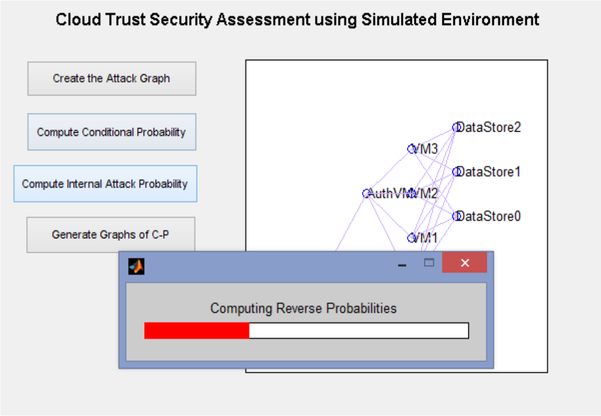
Figure shows a data center with devices connected in a hierarchical order. The devices are a Router, a Firewall, an Authorization VM which also acts as a load balancer, 4 VMs which are actual servers and 3 data-stores which are shared byall VMs. The lines show the connection of each device to the each other. It can be understood that the links are virtual links which are created in a cloud environment using virtual network interface. This VM architecture is used for serving some sensitive files. Each level can be considered as depth or level. Each level has its own security level. This security level will define the attack probabilities if previous level has been compromised.


Cloud Trust Security Assessment using Simulated Environment
Create the Attack Graph
Compute Conditional Probability
Compute Internal Attack Probability
Generate Graphs of C P
DataStore2
VM3
DataStore1
AuthVM
VM2
DataStore0
VM1

Computing Probabilities

Fig 4: *Computing the Conditional Probability*

In figure 4, we can see the computational probabilities are computed. Conditional probability is an important security assessment parameter in case of cloud security. We can consider conditional probability as P (B|A) which simply means the probability of occurrence of event B given that event A has already occurred. Such conditional probabilities allow us to assess the system security at each depth or level is given that the security at previous level is compromised.



Cloud Trust Security Assessment using Simulated Environment

Computing Reverse Probabilities

***Fig 5:** Computing the internal attack Probability*

In figure 5, we can see the internal attack probabilities are computed. Internal attack probability is an important security assessment parameter in case of cloud security. We can consider internal probability as P (B|A) which simply means the probability of occurrence of event B given that event A has already occurred. Such conditional probabilities allow us to assess the system security at each depth or level is given that the security at previous level is compromised.

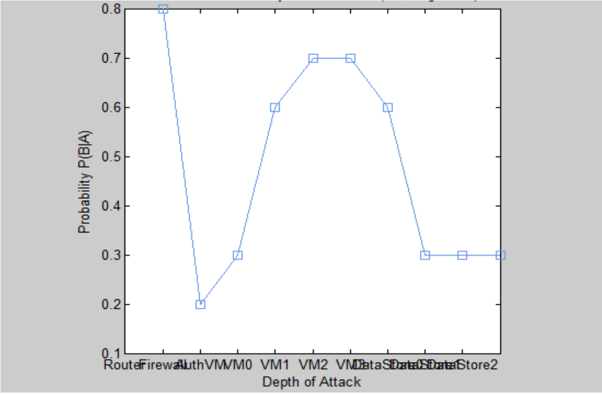


***Fig 6:** graph of conditional probability*

Figure 6 shows the graph of conditional probability i.e. the probability of occurrence of event B given that event A has already occurred. The graph shows that the security at first level is very weak (router level) and that the probability of it having been compromised is very high (0.8 or 80%). The second layer is the firewall and as assumed, the firewall has a very high level of security factor build into it and thus the probability that the firewall is compromised given that router has compromised is very low (0.2 or 20%). The other level which is very secure is Authorization VM and it is also providing a level of security with only 30% probability of being compromised given that level 1 and 2 are compromised. After this step is the three VMs and based on their security level each has a different probability of being compromised given that level 1, 2 and 3 are being compromised. At last, we have the data-stores. Since data stores mostly use VM level auth for data security and key based encryption for data access, these are still secure than VMs given that the all the levels 1, 2, 3 and 4 are compromised. The graph tells a lot about the security assessment of the system from an outsider attack as well as from insider attack in case an insider attack occurs.

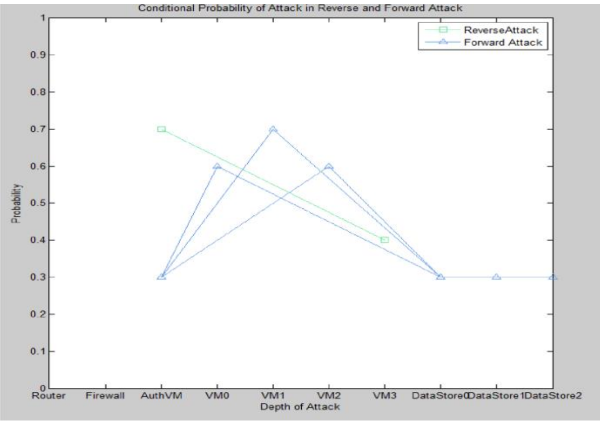


***Fig 7:** Conditional probability of attack in reverse and forward attack*

Figure 7 shows the graph of attack in reverse and forward attack in which conditional probabilities are shown as outside attack and inside attack. The forward attack is outside attack which is done from the first node to the next e.g. form router to firewall, firewall to auth vm and next. In reverse attack, the attacker has already the permission to use the VM and the other sources. For reverse attack, the attacker uses the malicious data to compromise the reverse level for use the other levels. So, if a user is using the one VM and he want to compromise the other VM then he needs to first attack Auth VM. If Auth VM is compromised he can compromise the other VM.

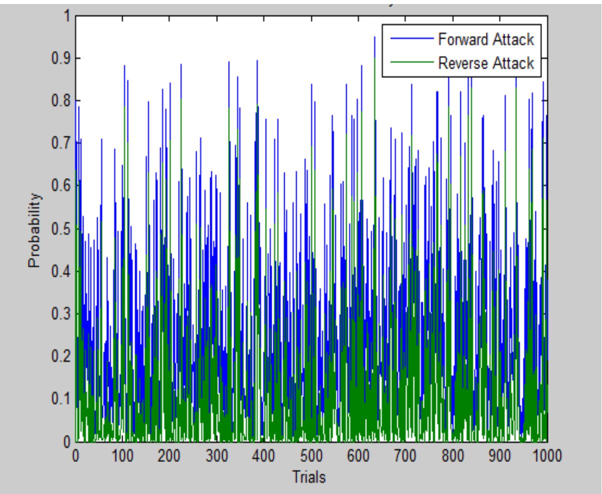
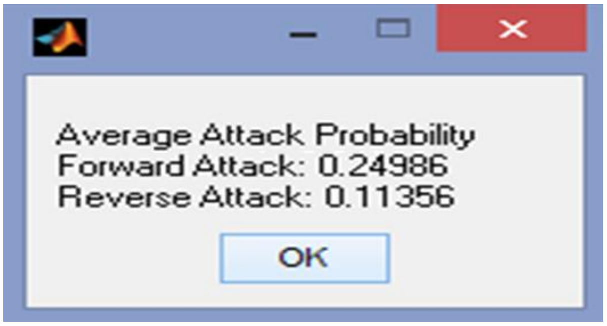


***Fig 8:** Graph of 1000 trials used by user*

Figure 8 shows the result of the 1000 trials or requests used by the user to use the Auth VM or the VM. In this graph, the green graph represents the attack probability of the reverse attack and the blue lines show the attack probability of the forward attack. These probabilities are calculated after compromises the one node if attacker attacks and compromise the firewall then assessment model will calculate the probability of an attack on the next level.



Average Attack Probability
Forward Attack: 0.24986
Reverse Attack: 0.11356

Fig 9: *result of average attack probability*

Figure 9 shows the result of forward and reverse attack probabilities. In which forward attack result is higher than reverse attack.

TABLE 3 *Comparison of Results*

Parameter	Previous (Forward Attack)	Proposed (Reverse Attack)
Average Attack Probability	0.24986	0.11356

From table 3 it has been concluded that result of proposed methods is better than last using model. In previous method forward attack probability is used but, in this method, we use both reverse and forward attack probabilities to compare results. By using this method, we can find and cover security holes and weak structures in cloud computing environment. Another benefit of this method it also able to detect APTs.

6 CONCLUSION AND FUTURE SCOPE

Trust Assessment is getting key priority with the growth of cloud service providers that take and store user data in their Data warehouses. Trust assessment provides the user with a level of trust in the provider as enterprise and user data security is a key parameter. Various trust assessment models have been developed, each having a different way to define trust etc. In this review, we have looked upon at various trust assessment models namely, Cloud-Trust, MTCEM, ENISA, and QUIRC. Each model has different key advantages and user base. Cloud-Trust provides a ground level bare metal security assessment scheme. MTCEM provides an enterprise as well as cloud administrator a peek at cloud security by providing multi-tier support. ENISA provide the assessment based on system policy and legal aspect of it. QUIRC is based on a mixed probability model to assess risk analysis. Although each has a mixed advantage, none of the models directly addresses Insider attack and its potential vulnerability assessment. This leaves us to develop a model that addresses this issue so this model is developed which can assess the inside threats as well as the forward attacks.Potential next steps should be to extend Cloud-Trust to Platform as a Service (PaaS) and Software as a Service (SaaS) CSPs. It would also be useful to develop a full set of data exfiltration APT attack steps that span the component space of CCSs and CSPs. It would also be to explore how CVSS data could be used to estimate APT attack probabilities. A robust sensitivity analysis methodology could also be developed to see which nodes and edges Cloud-Trust results are most sensitive to.

REFERENCES

[1] Te-Shun Chou, “Security threats on cloud computing vulnerabilities” International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, 2013

[2] Mohammed M. Alani, “Securing the Cloud: Threats, Attacks and Mitigation Techniques” International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, 2013

[3] Gerhard Eschelbeck et al. “Security Threat Report” Sophos and Sophos, 2012.

[4] Ramkumar.et.al, “Towards A Theory of Insider Threat Assessment”, IEEE International Conference on Dependable Systems and Networks 2005.

[5] Shital P. Adkine, “Security Analysis of Cloud Computing” International Journal of Computer Science and Informatics Vol 1, No 4, 2012

[6] Makhdoom Muhammad Naeem, et al. “An overview of virtualization and cloud computing” Science international Vol 4, No 28, 2016

[7] Seccombe A, et al. “Security guidance for critical areas of focus in cloud computing” v2.1. Cloud Security Alliance, 2009.

[8] Attanasio CR, “Virtual machines and data security” Proceedings of the workshop on virtual computer systems. USA: 1973. Pages. 206–209.

[9] Descher M, et al. “Retaining data control to the client in infrastructure clouds”. IEEE International conference on availability, reliability and security, 2009.

[10] Dan Hubbard, Websence “Top threats to cloud computing” Cloud security alliance Version 1.0, 2010

[11] Gonzales D et al. “Cloud-Trust - a Security Assessment Model for Infrastructure as a Service Clouds”, IEEE Transactions on Cloud Computing, 2015.

[12] Xiao Yong Li, Li Tao Zhou, Yong Shi, and Yu Guo, "A trusted computing environment model in cloud architecture," 9th International Conference on Machine Learning and Cybernetics (ICMLC), vol. 6, Qingdao, China, 2010, Pages. 2843-2848.

[13] Alessandro et al. “Report on Cloud Computing Security Risk Assessment. risk-assessment” The European Network and Information Security Agency, 2009

[14] Prasad Saripalli, et.al, “QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security” IEEE 3rd International Conference on Cloud Computing, 2010.

[15] Rizwana Shaikh et al. “Trust Model for Measuring Security Strength of Cloud Computing Service” International Conference on Advanced Computing Technologies and Applications, 2015

[16] Sudharsan Sundararajan et al. “Preventing Insider Attacks in the Cloud” Part I, CCIS 190, pp. 488–500, 2011.