Intrusion Detection and Prevention System for Cloud Simulation Environment using Hidden Markov Model and MD5

Harsha Banafar
M.Tech CSE
OIST Bhopal (MP)

Sanjay Sharma
Asst Professor
OIST Bhopal (MP)

ABSTRACT
Any activity aimed at disrupting a service or making a resource unavailable or gaining unauthorized access can be termed as an intrusion. Intrusion detection systems (IDSs) play a key role in detecting such malicious activities and enable administrators in securing network systems. The cloud computing platform gives people the opportunity for sharing resources, services and information among the people of the whole world. In private cloud system, information is shared among the persons who are in that cloud. For this, security or personal information hiding process hampers. In this paper we have proposed new security architecture for cloud computing platform. This ensures secure communication system and hiding information from others by authentication using shared secret key MD5 and provides security using Hidden Markov Model. This structure can be easily applied with main cloud computing features, e.g. PaaS, SaaS and IaaS. Our work mainly deals with the security system of the whole cloud computing platform.

Keywords
Cloud Computing, Intrusion detection and prevention system, MD5 Hashing, Hidden Markov Model.

1. INTRODUCTION
CLOUD computing technology is a service-based, Internet-centric, safe, convenient data storage and network computing service. It is an internet-based model for enabling a convenient and on-demand network access to a shared pool of configurable computing resources. The provision of various services over internet is possible through this technology which connotes software, hardware, data storage and infrastructure. Cloud computing service provider delivers the applications via internet. These services are accessed from web browsers, desktop and mobile apps. Cloud Computing Technologies are grouped into 4 sections which include SaaS, DSaaS, IaaS and PaaS. SaaS (Software as a Service) is an on-demand application service. It delivers software as a service over the Internet. It eliminates the need of installing and running the application on the customer's own computers. PaaS (Platform as a Service) is an ondemand platform service to host customer application. DSaaS (Data Storage as Services) is an ondemand storage service. IaaS (Infrastructure as a Service) is an on- demand infrastructure service. It delivers the computer infrastructure – typically a platform virtualization environment – as a service, along with raw (block) storage and networking. In order to make a secure usage of the services provided by the cloud, cloud authentication systems can use different password techniques like: i) Simple text password ii) Graphical password and iii) 3D password object. But each of this has its own drawbacks.

Intrusion Detection System
An intrusion-detection system (IDS) can be distinct as tools, solution, and resources used to help identify, assess, and to claim unconstitutional or unapproved network action. Intrusion detection is characteristically one part of an overall fortification system that is installed around a system or device it is not a stand-alone protection measure. An intrusion detection system (IDS) is an indispensable part in a good network security background. It enables detection of suspicious packets and attacks. With the help of IDs, all network traffic can be observed.

Conventional intrusion detection systems (IDS) in wired networks analyse the behaviour of the elements in the network trying to identify anomalies produced by intruders and, once identified, start a response against the intruders. These detection systems are usually placed in those elements with more confluent traffic such as routers, gateways, and switches. Unfortunately, in ad-hoc networks, those elements are not uses, and it is not possible to guess which nodes will route more traffic from its neighbours and install IDS systems only in those nodes .

Intrusion detection techniques are traditionally categorized into two methodologies: anomaly detection and misuse detection. Anomaly based intrusion detection systems base their decisions on anomalies, belongings that do not usually occur. Misuse detection seizes intrusions in terms of the characteristics of known attacks or system vulnerabilities; any action that conforms to the pattern of a known attack or vulnerability is considered intrusive.

The components of Intrusion Detection System can be of three types.

Network intrusion detection
Network intrusion detection systems listen to network communications. They are acquainted with intrusions which come during the networking environment. Essentially a network intrusion detection system (NIDS) is a service which listens on a network interface looking for suspicious traffic. Network intrusion detection systems are mostly signature based.

Host Based Intrusion Detection
Host intrusion detection systems (HIDS) inhabit on a resource supervised. This resource is mostly a computer server or workstation. HIDS seem at produced log files, changes in the file system or check for changes in the process table. Their objective is to identify intrusions into a host.

Signature based intrusion detection

Signature based intrusion is based on signatures of known attacks. These signatures are accumulated and evaluated against events or received traffic. If a pattern matches, an alert is generated.

Issues in Cloud Data Storage

Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud.

A. Trust: Trust is defined as reliance on the integrity, strength, ability and surety of a person or thing. Entrusting your data on to a third party who is providing cloud services is an issue. Recent incidents like In April of 2012 Amazon's Elastic Compute Cloud service crashed during a system upgrade, knocking customers' websites off-line for anywhere from several hours to several days. That same month, hackers broke into the Sony PlayStation Network, exposing the personal information of 77 million people around the world. And in June a software glitch at cloud-storage provider Dropbox temporarily allowed visitors to log in to any of its 25 million customers' accounts using any password or none at all. These issues have certainly created doubts in mind of cloud consumers and damaged the trust ability of Consumers.

B. Privacy: Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users.

C. Security: Cloud service providers employ data storage and transmission encryption, user authentication, and authorization. Many clients worry about the vulnerability of remote data to criminals and hackers. Cloud providers are enormously sensitive to this issue and apply substantial resources to mitigate this problem.

D. Ownership: Once data has been relegated to the cloud, some worry about losing their rights or being unable to protect the rights of their customers. Many cloud providers address this issue with well-skilled user-sided agreements. According to the agreement, users would be wise to seek advice from their favourite legal representative.

E. Performance and Availability: Business organizations are worried about acceptable levels of performance and availability of applications hosted in the cloud.

F. Legal: There are certain apprehensions for a cloud service provider and a client receiving the service like location of the cloud provider, infrastructure and physical location of the data and outsourcing of the cloud provider's services etc.

***G. Multiplatform Support*:** More an issue for IT departments using managed services is how the cloudbased service integrates across different platforms and operating systems, e.g. OS X, Windows, Linux and thinclients. Usually, some customized adaption of the service takes care of any problem. Multiplatform support requirements will ease as more user interfaces become web-based.

H. Intellectual Property: A company invents something new and it uses cloud services as part of the invention. Is the invention still patentable? Or there can be issues like cloud service provider can make claim for that invention or leak the information to the competitor.

I. Data Backup: Cloud providers employ redundant servers and routine data backup processes, but some people worry about being able to control their own backups. Many providers are now offering data dumps onto media or allowing users to back up data through regular downloads.

J. Data Portability and Conversion: Some people have concerns like, switching service providers; there may be difficulty in transferring data. Porting and converting data is highly dependent on the nature of the cloud provider's data retrieval format, particular in cases where the format cannot be easily revealed. As service competition grows and open standards become established, the data portability issue will ease, and conversion processes will become available supporting the more popular cloud providers. Worst case, a cloud subscriber will have to pay for some custom data conversion.

These are certain areas in which cloud computing requires to excel and solve problem related to it. Out of all the problems Security, Privacy and Intellectual property put the major threats on growth of cloud computing that are needed to be worked upon.

Objective

Paper objective is to provide security of two types:

a.) It provide authentication from unauthorized user using MD5 (Message Digest 5).

b.) It also provide security for authorized user who store their data in Cloud Data center and some authorized user try to misuse secure data. It is provided by using HMM (Hidden Markov Model)

Distinctive Feature

As we know that three types of intrusion is possible: Masquerader (unauthorised user attack),Misfeasor (authorised user attack) and clandestine user(who seizes control of system) This paper will provide security of all types of attacks.

First it create cloud environment. As soon as environment is created it analyzes cloud datacenter,virtual machine as well as cloud user. When user want to store data or access from datacenter it first define identity of user using MD5. After that data is send by define probabily of states using HMM. Intrusion is finds by value of probability.if it is greater than threshold then it is said intrusion is detected after that prevention is done otherwise it is not intrusion.

2. RELATED WORK

Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem [1]-In this paper they have proposed new security architecture for cloud computing

platform. This ensures secure communication system and hiding information from others. AES based file encryption system and asynchronous key system for exchanging information or data is included in this model.This structure can be easily applied with main cloud computing features, e.g. PaaS, SaaS and IaaS. This model also includes onetime password system for user authentication process. environment for the access of data or in case of data integrity.But the architecture of the cloud implemented so far doesn't provide right access permission of one data to another. The model is not authentic and also the chances of attacks have been possible which increases the resource utilization.

Sung-Bae Cho and Hyuk-Jang Park [2]-In This paper proposes an effective HMM-based intrusion detection system that improves the modeling time and performance by only considering the privilege transition flows based on the domain knowledge of attacks.A hidden Markov model (HMM) is a useful tool to model sequence information, an optimal modeling technique to minimize false-positive error while maximizing detection rate.

Dinesha H A and Dr.V.K Agrawal[3]-In this paper, they are proposing the strong password generation technique by considering multiple input parameters of cloud paradigm referred as a multidimensional password. Cloud computing is drastically growing technology which provides an on-demand software, hardware, infrastructure and data storage as services. This technology is used worldwide to improve the business infrastructure and performance. However, to utilize these services by intended customer, it is necessary to have strong password authentication. At present, cloud password authentication can be done in several ways, such as, textual password, graphical and 3D password.

Siva S. Sivatha Sindhu, S. Geetha , A. Kannan [4]-The objective of this paper is to construct a lightweight Intrusion Detection System (IDS) aimed at detecting anomalies in networks. Therefore in this work, the design of IDS is investigated from these three perspectives. The goals of this paper are (i) removing redundant instances (ii) identifying suitable subset of features by employing a wrapper based feature selection algorithm (iii) realizing proposed IDS with neuro tree to achieve better detection accuracy. The lightweight IDS has been developed by using a wrapper based feature selection algorithm that maximizes the specificity and sensitivity of the IDS as well as by employing a neural ensemble decision tree iterative procedure to evolve optimal features.

R Rangadurai Karthick,Vipul P. Hattiwale, Balaraman Ravindran [5]-In this paper they describe an adaptive network intrusion detection system, that uses a two stage architecture. In the first stage a probabilistic classifier is used to detect potential anomalies in the traffic. In the second stage a HMM based traffic model is used to narrow down the potential attack IP addresses.

Richa Sondhiya, Maneesh Shreevastav, Mahendra Mishra[6]-In this paper, they propose a method that enables cloud computing system to achieve both effectiveness of using the system resource and strength of the security service without trade-off between them. In this paper,they propose a soft Computing technique such as MLP Algorithm for detecting the unknown intrusion in network intrusion detection in cloud computing environment. As we know that Cloud computing is a new type of service which provides large scale computing resource to each customer. Cloud Computing Systems can be easily threatened by various cyber-attacks, because most of Cloud computing system needs to contain some Intrusion Detection Systems (IDS) for protecting each Virtual Machine (VM) against threats. In this case, there exists a tradeoff between the security level of the IDS and the system performance. If the IDS provide stronger security service using more rules or patterns, then it needs much more computing resources in proportion to the strength of security. So the amount of resources allocating for customers decreases. Another problem in Cloud Computing is that, huge amount of logs makes system administrators hard to analyze them.

Mohit Marwaha, Rajeev Bedi[7] -This paper analyzes the feasibility of the applying encryption algorithm for data security and privacy in cloud Storage. Cloud computing is an Internet-based computing technology, in which software, shared recourses and information, are provided to consumers and devices on-demand, and as per users requirement on a pay per use model. Even though the cloud continues to grow in popularity, Usability and respectability, Problems with data protection and data privacy and other Security issues play a major setback in the field of Cloud Computing. Privacy and security are the key issue for cloud storage. Encryption is a well known technology for protecting sensitive data. Use of the combination of Public and Private key encryption to hide the sensitive data of users, and cipher text retrieval.

Kashif Munir and Sellapan Palaniappan[10] - The biggest challenge in cloud computing is the security and privacy problems caused by its multi-tenancy nature and the outsourcing of infrastructure, sensitive data and critical applications. Enterprises are rapidly adopting cloud services for their businesses, measures need to be developed so that organizations can be assured of security in their businesses and can choose a suitable vendor for their computing needs. The boom in cloud computing has brought lots of security challenges for the consumers and service providers. How the end users of cloud computing know that their information is not having any availability and security issues?

In this paper they identify the most vulnerable security threats/attacks in cloud computing, which will enable both end users and vendors to know about the key security threats associated with cloud computing and propose relevant solution directives to strengthen security in the Cloud environment. They also propose secure cloud architecture for organizations to strengthen the security.

Flavio Lombardi a, Roberto Di Pietro[11]-Cloud computing adoption and diffusion are threatened by unresolved security issues that affect both the cloud provider and the cloud user. In this paper, we show how virtualization can increase the security of cloud computing, by protecting both the integrity of guest virtual machines and the cloud infrastructure components. In particular, we propose a novel architecture, Advanced Cloud Protection System (ACPS), aimed at guaranteeing increased security to cloud resources. ACPS can be deployed on several cloud solutions and can effectively monitor the integrity of guest and infrastructure components while remaining fully transparent to virtual machines and to cloud users. ACPS can locally react to security breaches as well as notify a further security management layer of such events. A prototype of our ACPS proposal is fully implemented on two current open source solutions: Eucalyptus and OpenECP. The prototype is tested against effectiveness and performance. In particular: (a)effectiveness is shown testing our prototype against attacks known in the literature; (b)performance evaluation of the ACPS prototype is carried out under different types of workload. Results show

that our proposal is resilient against attacks and that the introduced over head is small when compared to the provided features.

3. PROPOSED TECHNIQUE

This provides the security of two types:

a. Inside the cloud(within cloud environment)

b. Outside the cloud (outsise cloud environment)

This model provides security in two steps:

Step 1: In first step in checks authentication of user. If it is valid user then user can enter in cloud environment otherwise it cannot enter in cloud environment.

Step 2: If user is valid user it enter in the cloud environment and send and retrieve data to DataCenter. After that following method is done:

Methodology

1. Create cloud simulation environment consisting of dynamic number of users and datacenters.
2. As soon as the cloud is established the sender can send packets to the datacenter.
3. Now initialize the HMM with certain parameters at server or broker level of the cloud.
4. The number of states in the model will depends on the users in the cloud.
5. As soon as the packets start sending from user to datacenter, HMM starts calculating the probability of each of the packet in the transition state.
6. If the probability of packet exceeds threshold value then a detector is started to detect the intrusion in the packet.

Markov Model

A **Markov process** is a stochastic process (random process) in which the probability distribution of the current state is conditionally independent of the path of past states, a characteristic called the Markov property.

Markov Property: The state of the system at time t+1 depends only on the state of the system at time t

Hidden Markov Models (HMMs) are used for situations in which:

The data consists of a sequence of observations

The observations depend (probabilistically) on the internal state of a dynamical system.The true state of the system is unknown (i.e., it is a hidden or latent variable).

The Need for Authentication

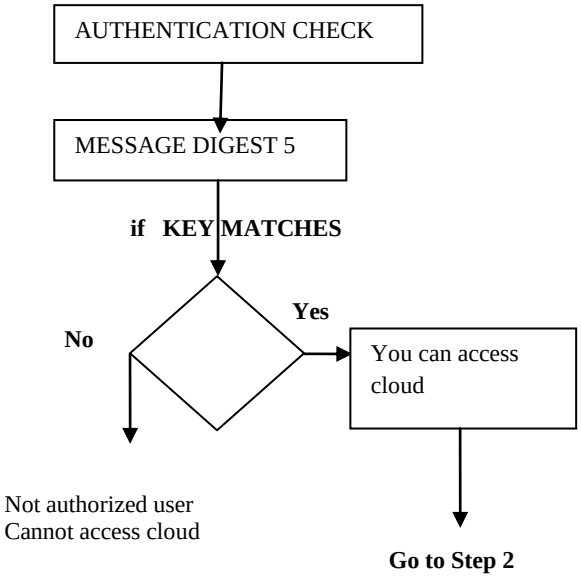
Message Authentication is the procedure to verify that the received message come from alleged source and have not altered.We want to verify the identity of who we are communicating with. We want to ensure that what they sent is what we received (integrity). We don't want to allow unauthorized registrations.

MD5

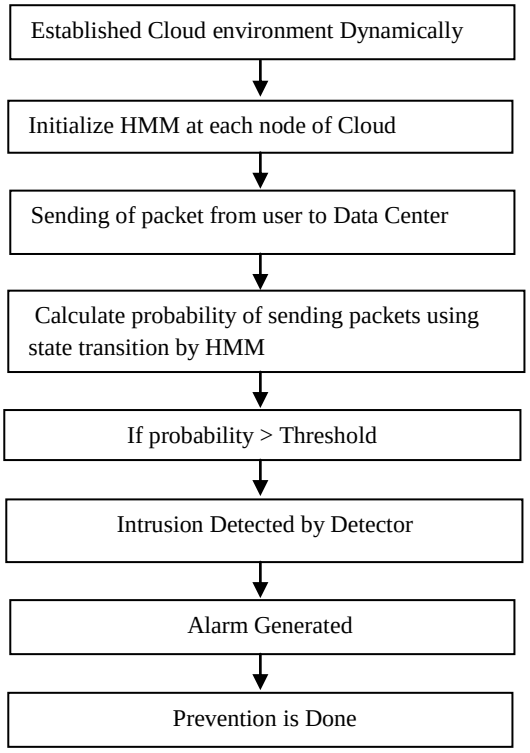
MD5 algorithm was developed by Professor Ronald L. Rivest in 1991. According to RFC 1321, "MD5 message-digest algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input …The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA".

3.1 Working Model

STEP 1:



STEP 2:



3.2 Algorithm

Detection of intrusion:

A Hidden Markov Model contains five tupples:

N – is the number of states in the model Q {Q1, Q2, Q3,….}.
M – is the number of observation symbols V {V1, V2, V3…..}.

A – State transition Probabilities
B – is the distribution of each of the states
Π – is the initial state distribution

1. The initial transition probability from one state Q1 to another state Q2 at a particular instance of time t+1 depends on the state at time t according to the assumption of markov i.e.
$$a_{ij} = p(q_{t+1} = s_j \mid q_t = s_i)$$
2. The probabilities of the transition of the states is independent of the actual time where the transition takes place according to the assumption of stationarity i.e.
$$p(q_{t+1} = s_j \mid q_{t1} = s_i) = p(q_{t2+1} = s_j \mid q_{t2} = s_i)$$
3. Lets 'n' is the number of packets 'pkt' send at a particular transition at a particular instance of time.
4. Calculate each step of the transition the state which is most probable $\hat{q}_i, 1 \le i \le T$ for the observation $z_i, 1 \le i \le T$, probability of state transition δt can be computed using viterbi algorithm.
5. After each step of the transition calculate the general probability of the packet to be transmitted at each step Q.
6. The average probability can be computed using
$$\delta_{avg}=(\sum_{k=1}^{T}\delta_k^{(i)})/_T$$
7. The condition is checked i.e. if the average probability is less than the threshold value then the intrusion is detected in the packet.
$$\delta_{avg} < \text{(initial threshold value)}$$

Prevention of intrusion

The prevention of the intrusion in the cloud environment can be prevented by increasing average threshold of the transition states of the packets of the packets 'pkt'.

1. The initial transition probability from one state Q1 to another state Q2 at a particular instance of time t+1 depends on the state at time t according to the assumption of markov i.e.
$$a_{ij} = p(q_{t+1} = s_j \mid q_t = s_i)$$
2. The probabilities of the transition of the states is independent of the actual time where the transition takes place according to the assumption of stationarity i.e
$$p(q_{t+1} = s_j \mid q_{t1} = s_i) = p(q_{t2+1} = s_j \mid q_{t2} = s_i)$$
3. Lets 'n' is the number of packets 'pkt' send at a particular transition at a particular instance of time.
4. Calculate each step of the transition the state which is most probable $\hat{q}_i, 1 \le i \le T$ for the observation $z_i, 1 \le i \le T$, probability of state transition δt can be computed using viterbi algorithm.
5. After each step of the transition calculate the general probability of the packet to be transmitted at each step Q.
6. The average probability can be computed using
$$\delta_{avg}=(\sum_{k=1}^{T}\delta_k^{(i)})/_T$$
$$\delta_{avg}=(\sum_{k=1}^{T}\delta_k^{(i)})/_{T+1}$$
7. The condition is checked at each node of the cloud means the next state and the previous state of the transition i.e. if the average probability is less than the next average threshold value then the packets is transferred from the next other transition state.

4. PROBLEM STATEMENT

Although there is any authentication techniques implemented in the cloud environment for the access of data or in case of data integrity.But the architecture of the cloud implemented so far doesn't provide right access permission of one data to another. The model is not authentic and also the chances of attacks have been possible which increases the resource utilization.

5. CONCLUSION

Security plays a vital role during the transmission of data from one node to the other. The data integration among various clouds and data access from one cloud to other is simple but authentication for the access of data is necessary so that the number of attacks is reduced. The proposed model implemented here provides a simple and efficient way of data integrity and the access of data in a cloud environment.

6. FUTURE WORK

Although the intrusion detection using HMM provides efficient results but further enhancements can be done in the field of power consumption in the cloud computing when the data is stored in the data centers.

As well as we know that cloud computing is widely use, that's why security is main issue in cloud computing. Further enhancement can be done in the field of cloud computing security.

7. ACKNOWLEDGMENTS

It is my immense pleasure to express my deep sense of gratitude and indebtedness to my highly respected and esteemed Mr. Sanjay Sharma, and Mrs. Shreeja Nair HOD (CSE) OIST, Bhopal. His invaluable guidance, inspiration, constant encouragement sincere criticism and sympathetic attitude could make this paper possible.

8. REFERENCES

[1] Kawser Wazed Nafi , Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012.

[2] R Rangadurai Karthick,Vipul P. Hattiwale, Balaraman Ravindran "Adaptive Network Intrusion Detection System using a Hybrid Approach" 978-1-4673-0298-2/12/$31.00 c 2012 IEEE.

[3] Siva S. Sivatha Sindhu , S. Geetha , A. Kannan "Decision tree based light weight intrusion detection using a wrapper approach" Expert Systems with Applications 39 (2012) journal homepsage: www.elsevier.com/locate/eswa.

[4] Sung-Bae Cho and Hyuk-Jang Park "Efficient anomaly detection by modeling privilege flows using hidden Markov model" Computers & Security Vol 22, No 1, pp 45-55, 2003

[5] Dinesha H Aand Dr. V.K Agrawal "MULTI-DIMENSIONAL PASSWORD GENERATION TECHNIQUE FOR ACCESSING CLOUD SERVICES" International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.2, No.3, June 2012.

[6] Md Kausar Alam, Sharmila Banu K "An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds"International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 ISSN 2250-3153 www.ijsrp.org .

[7] Mohit Marwaha, Rajeev Bedi "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing"IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013 ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814 www.IJCSI.org.

[8] Richa Sondhiya, Maneesh Shreevastav, Mahendra Mishra "To Improve Security in Cloud Computing with Intrusion detection system using Neural Network" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013.

[9] Ms.Asha.D and R.Chitra "Securing cloud from ddos attacks using intrusion detection system in virtual machine" IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013 ISSN: 2320 - 8791

[10] Kashif Munir and Sellapan Palaniappan "Security Threats/Attacks Present in Cloud Environment".

[11] Flavio Lombardi, Roberto Di Pietro "Secure virtualization for cloud computing" Journal of Network and Computer Applications 34 (2011) 1113–1122.

[12] Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande "Intrusion Detection System for Cloud Computing" International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012 ISSN 2277-8616 67 IJSTR©2012

[13] Yizhang Guan, Jianghong Bao "A CP Intrusion Detection Strategy on Cloud Computing" ISBN 978-952-5726-00-8 (Print), 978-952-5726-01-5 (CD-ROM) Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09).

[14] Aerohive Network white paper "The Benefits of Cloud Networking" Enable cloud networking to lower IT costs & boost IT productivity

[15] Veselina Jecheva "About Some Applications of Hidden Markov Model in Intrusion Detection Systems" International Conference on Computer Systems and Technologies - *CompSysTech'06*

[16] Issa M. Khalil , Abdallah Khreishah and Muhammad Azeem "Cloud Computing Security: A Survey" Computers2014,3,1-35; doi:10.3390/computers3010001 computers ISSN 2073-431X www.mdpi.com/journal/computers

[17] Andre Arnes, Fredrik Valeur, Giovanni Vigna, and Richard A. Kemmerer "Using Hidden Markov Models to Evaluate the Risks of Intrusions" System Architecture and Model Validation.

[18] Nong Ye "A Markov Chain Model of Temporal Behavior for Anomaly Detection" Proceedings of the 2000 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 6-7 June, 2000 $10.00 © 2000 IEEE 171.