RESEARCH ARTICLE OPEN ACCESS

Honey pot based new algorithm for data security

Apurva Saxena[1], Dr.Pratima Gautam[2], Dr. Anubha Dubey[3]
[1]Research Scholar (Computer Science Engineering), Rabindranath Tagore University, Bhopal, India
[2] Dean of Computer Science and Application, Rabindranath Tagore University, Bhopal, India
[3]Independent researcher and analyst, Bioinformatics Bhopal, India
Corresponding Author: Apurva Saxena

ABSTRACT
Cloud computing an emerging technology provides various services to the users like infrastructure, hardware, software, storage etc. So, it is necessary that cloud computing network should always free from attack. Various strict security checking systems are used for making network bugs free and honey pot is among one of the tool that is used to provide security. Various models are proposed for honey pot to solve the problem of industries and that is used to captures the activities of attackers and maintains a log for providing better security to the cloud network. Here in this paper we proposed an algorithm to resolve some of the issues of network security**.**
Keywords: Cloud computing, honey pot, virtual machine

Date of Submission: 20-12-2018 Date of Acceptance: 04-01-2019

I. INTRODUCTION

Cloud computing is a centralized controlling system in which minimal resources are offered by the providers, due to which intruder easy gain access to the resources and breach the security. Cloud computing allows the user to take benefit of the technologies. It is used for delivery of its services like-servers, storage, databases, [5] networking, software, analytics and many more. It is agile for the organization in improving the services provided to the user. One of the foremost characteristics of the cloud computing by which it provides flexibility to the user through the reduction of cost. Other one cloud computing services is speed which is provided to self service and on demand large amount of computing resources transfer within a minute without any pressure of capacity planning. Here cloud knew at which time how much amount of power, bandwidth and storage is required according to the geographic conditions [6]. By using on-time data centers in computing productivity gets increases. It becomes more reliable as it secures data, disaster recovery. Types of cloud services are IaaS (Infrastructure as a Service) in this customer can get infrastructure and virtual machine, networks on rent. PaaS (Platform as a Service) it is designed to make a platform for the user to develop a web or mobile apps without applying setup behind it. SaaS (Software as a Service) it is designed to develop a software on demand for the user. Cloud provider host and manages the application, underlying infrastructure and handle maintenance too. There are three different ways to deploy cloud computing like-public, private and hybrid cloud. Virtualization is the new technology of the cloud computing. This technology divided physical computers into virtual devices by which they can easily manage the task. Generally cloud provider is using traditional security system to avoid authorized access of the resources. Virtualization is a key point in the cloud system that provides multiple virtual instance of a physical resource and if a single instance of a resource susceptible then connected clients are affected [7]. Honeypot is a very simple technique and always keep the information in small parts. It gives the security to the network by using encryption technique. If any attacker tries to invade or penetrate in the network by connecting this technique honeypot will trap, detect and trace its activities. It is designed in such a way that if anything thrown at them will capture whether it may be tool or strategy. As honeypot is a source of information system, it comprises of data, computers and segments of network. It has a special feature of continuous monitoring the behavior of the hacker/attacker and requires minimal resources to trace the activity. Honeyd is an open source honeypot application that keeps virtual host on network. It's a type of a low interaction honeypot which perform services like FTP, HTTP.

Honeypot can be classified into two different types [8]:

1 Production Honeypot: - It's a type of low interaction honeypot, which is easy to use and has only limited information about the hacker's reroute and justifying his attacks. It is applied in business corporations and organization.
2 Research Honeypot: It gives detail information about the strategy and motives of the attacker. It

is complex to implement and mainly used in military, research and government organization.

Honeypots are classified into different ways like:

- Low-interaction Honeypots: It requires only one physical machine. This honeypot gives the information about the attacker who is frequently access the network. They use only few resources on the multiple virtual machines with a small response time. It requires less code by which complexity of security gets reduced.
- Medium-interaction Honeypot: In this attacker is not in communication with real system. This honeypot did not gives you detail information about the hacker. It gives partial service as compare to low-interaction honeypot.
- High-interaction Honeypot: It works on isolated network on which hosts variety of services. It gives the maximum amount of attacker's information activities when interact with our system. This technique is implementing on one physical machine per honeypot which direct increase the cost and maintenance. It is complex to install but security is an issue.

Honey pot gives us valuable information about the attacker's action [9]. The honeypot is a system or computer who sacrifices themselves to target the attacker of hackers. The aspire of the Honey pot is investigating, understanding, watching and tracking hackers perspective in order to create a protected system by its different behavior as follows:

A. Analyzing intruder behavior using Honey pot – Honey pot is a system on network is used to trap, monitor an identifier the suspicious request in the system. It is actually a tool to collect the evidence or behavior about hacker and their attacking methodology. By this we redirect the attacker or hacker from the actual setup of the network to the virtual system[10].Various honeypots techniques are exist like Dionaea, Kippo and Amun used in cloud platform.

Following are the steps by which any simulator work in the virtual environment in the cloud platform:-

1. Collecting the behavior of the intruder on the basis of certain parameters

Behavior of the intruders is collected on the basis of below given arguments which will be stored in the log table.

1.1 User IP address – Using simulator we can easily collect the IP address of the intruder IP.

1.2 Pattern recognition – Various intruders have different behavior like replicating the data and used for some intentionally designed network, editing the data, harm the network, damage the trust boundaries of the users etc.

1.3 Frequency of accessing the network or system – This is used to monitor the attempt of malicious user and calculating the frequency of accessing the network.

B. Encrypt the log table:

For providing enhanced security to our network, collecting data are stored in log table. It is also helpful for making different tools on the basis of the collected information. So it is necessary to store data in encrypted form in the network.

II. LITERATURE SURVEY

G.E.Blonder,1996[1],Dhamija et.al2000[2], X. Suo et.al2005[3] proposed a recognition-based graphical password system that authenticates users by choosing portfolios among decoy portfolios. He has discussed here many graphical password schemes have been proposed till now for securing data.

Paul. A.J, et.al 2007 [4] has presented security in cloud computing environment mostly uses right now infrastructure as a service for the research.

Joshi Ashay Mukundrao, et.al 2011[5], Hwan-Seok Yang, 2013[10],Muhammet Baykara, et.al 2015[13] explained that Cloud computing and Intrusion Detection and Prevention Systems are one such measure to lessen these attacks. Hybrid Intrusion Detection System (HIDS) that combines the positive features of two different detection methodologies. He has given many research projects from the past have built intrusion detection systems and honeypot architectures based on virtual machine introspection (VMI) are discussed.

Stephen Brown, et.al 2012 [7], Michael Beham ,et.al ,2013[9] given the proposed project they conducted a study using various honeypots (Dionaea, Kippo, and Amun)within different cloud computing platforms (such as Amazon EC2, Windows Azure etc.) with the objective of learning more about what kind of packets they receive networks.

Nithin Chandra et.al 2012[8], Ramya. R,cloud 2015 [14] presented a Cloud Security using Honey pots. The purpose of their research paper is to explain how honey pots are used for securing cloud systems, their advantages and disadvantages etc. She explained in this computing means accessing the data from data centers that reduces the chances of eavesdropping and storage cost. Sultan Aldossary, et.al 2016[15] and Gagan,et.al2016 [16] explained that Cloud computing change the entire world as necessity grows day by day by moving the data into cloud. Data stored in the cloud which is in virtual machine use to share resources in cloud. Yunfei CI, et.al 2017[17], Liangxuan Zhang,et.al 2017[18] explained that cryptography gives assurance to network and information security. In cryptography,

attribute based encryption (ABE) is one of the technique to protect the data.

2. Issues in network security:

In network security, number of techniques exist to detect malicious [14] user, misuse and abuse of computer systems by many types of intruders irrespective of any network they belong. Cloud computing is a drastically growing technology which provide services to users as per their demand. Many companies are migrating in the cloud computing environment but still have some security issues. For this reason we need to find a new tool to make data more secure and safe. Virtualization is one of the important component of the cloud computing. It provides an illusion of something like virtual computer, storage device, and network, hardware platform resources [13]. Some security issues are as follows with their possible solutions:-

1. A Cross Virtual Machine Side-Channel Attacks:-In this attacker attack through side-channel. Through the channel information get leaked by stealing the cryptographic key.
   Possible Solution:-[2] For security of the key if substitution method is applied in the key with two level securities like generate the OTP (One Time Password).
2. VM Image Sharing: - In this, threat is inside the image and forward it to others. By this act data can be leaked or it harm in many ways.
   Possible Solution: - [1] By sharing any image be alert and provide some security features like apply some cryptographic technique in encapsulate the image in the form of text and then share it.
3. VM Isolation: - In this single machine contains more than one virtual machine has its own guest operating system. If one operating system get fails other start work.
   Possible Solution: - Each VM in a single system has secured independently by anti-virus, so that by sharing hardware resources of the system.
4. VM Escape:-In this VMM (virtual machine manager) manages the data malicious user escape from [13] the manager from which it direct communicate with the host operating system.
   Possible Solution: - Whenever any unauthorized user try to interact with the host operating system the alarm generate to the manager in the form of pop-up message.
5. VM Migration: - In this when one migrate in the virtual machine from one host to another. It has some types like cold migration in this move the virtual machine from one data centre to another [15]. Second one is suspended virtual machine in this suspended virtual machine can migrate from one data centre to another. Another is migration with VMotion that allows moving from powered-on virtual machine to a new host. Last one is migrate with storage VMotion moves the virtual disk or configuration file of a powered-on virtual machine to a new data store.

   Possible Solution:-In all this process provides security at each level and when migration is in process rest all process should not be idle so that attacker must not be benefited.
6. VM Rollback:-This process gives more flexibility to the user. When VM rollback to the previous state but the state is not static, so when user gives the command of rollback they disable the previous state.

   Possible Solution: - In this always check the previous state it is correct, so try to validate the state.
7. Hypervisor Issues: - [16] Hypervisor or VMM (virtual machine monitor) hardware that creates and runs VM. The hypervisor run on host and having guest operating system. It manages the execution of the operating system and assigning the resources.

   Possible Solution: -Each VMM of the host must have some secure cryptographic techniques so the attacker should not get benefited.

As unauthorized activities are increasing quickly, Honey pot is an effective tool to find the behavior of the intruder who forcefully entered into the network with suspicious intention. Security has three important features which are prevention, detection and respond. Some security solutions consist of hardware and software components, whereas honeypot have two main features like detection and respond [18]. Existing techniques cannot provide complete protection against intruders, for example:

1 There are no prevention measures still existing for protecting the IP address on the network.

2 Most of the attack are currently observed on SSH and HTTP network. So there is a requirement to find counter measures to safe the network.

3 Hidden intruders are not easy to track which are making [17] DDOS (Distributed denial of service) attack in the network.

DDOS (Distributed Denial of Service) means making flood attack on a particular node by multiple nodes at the same time.

Therefore, in this paper we try to solve these issues by mentioning new proposed algorithm. Our newly proposed algorithm for data security in honey pot is that "On cloud computing platform every technique use to store the data needed good security system by creating virtualization".

Steps to follow our new algorithm are as follows:-

1. Identify and trap the privacy challenges in the network.
2. Improve the existing security issues.
3. Develop authentication tools and protocol at firewall level.
4. Enhance the security feature in the network using cryptography.

A. Analysis Of Algorithm

Here we have developed new algorithm on cloud computing platform, every technique use to store the data needed good security system. Data security is a challenging job in current cloud computing network, due to emerging attack of intruder which is not easy to track. Various threats existing in the cloud environment are data breaches, data loss, traffic hijacking, DDoS, Suspicious users, SQL injection attack, captcha breaking etc. There are many techniques by which data can be hack like unauthorized user access the data, share the[3] password, pin number, one time password by application scan the finger print. By recovering some security issues has some possible solution like sms alert or pop-up message should be on the smart phone if someone hack the data or protect the password or pin number by providing double security with the cryptographic method. This method can be applied at the firewall level of the network. This provides the dual security to the network, which is shown in figure1.

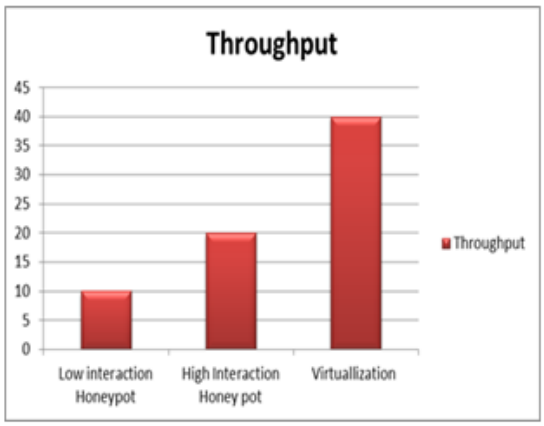

Figure1.Graph shows the throughput in different types of Honeypot and virtualization techniques.

It shows the throughput of the types of honeypot and virtualization. Here in low-interaction honeypot deals with the minimum system by which throughput of the system is get reduced. In high-interaction honeypot maintenance required for the system and security gets reduced by which throughput gets affected. In virtualization technique we try to work on all the factors (cost, security, maintenance and so on...), it becomes complex but throughput get increased.

B. Expected Outcome

According to our new proposed algorithm the computers are active on every attack of the hacker by penetrating into the deeper way. By this method of penetration administrator planned to have a continuous monitoring on the hacker's tricks and protect it by applying various techniques. Any malicious procedure done by intruder towards the authenticity of the data through the [8] honeypot, then these different types of honeypot technique record its activity and trap there it. By the use of this table1 we have taken different parameters like cost, maintenance, security and complexity applied on various types of honeypot and on our algorithm virtualization to get the overview.

Parameters	**Low Interaction**	**Medium Interaction**	**High Interaction**	**Virtualization**
Cost	NO	NO	YES	YES
Maintenance	NO	YES	YES	NO
Security	NO	YES	NO	YES
Complexity	NO	NO	NO	YES

Table1.This table shows the parameters on which different techniques depend.

As in the low interaction honeypot they need minimum system requirements so the network must be small, manageable and will be secured. In this they don't keep important and real data on the network. Now in the medium interaction honeypot it's a combination of low and high interaction

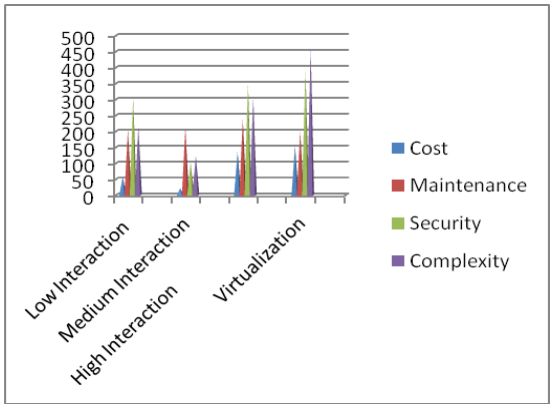

Figure2. This graph shows the impact of parameters on different types of Honeypots and virtualization.

honeypot in which attacker is not in direct communication with real data. As in high interaction honeypot system requirement is much high by which

requirement of maintenance is needed and cost is also increases. It works on isolated network security is not an issue but they are having simpler design so it get easily be attacked by hacker. In figure2 we show the effect of these factors (security, cost, maintenance, complexity) on these techniques so that we can increase our efficiency by working on them. This virtualization algorithm works on virtual environment (cloud sim, KFSensor, etc...) because of which gives the output in a desirable way.

One of the techniques is data breaches. In this type, attacker tries to acquire encryption key. Intruder always try to gain access of private cryptographic key. Hacker finds out the location of the company confidential data. Intruder accumulates various keys for taking control over sensitive data. But by having dual security feature like scanned images of finger print or thumb impression, data will be secure by virtualization environment.

III. CONCLUSION

Results of honey pot are used to capture the activities of hackers. Tools are being used for analyzing the behavior of the hacker. Logs are maintained and gather information which is helpful for the network administrator. Cloud computing is novel technology that provides easy computing and access to high performance computing, networking, storage and infrastructure through internet. Cloud computing have potential to provide high efficiency and cost savings. As cloud computing is the development trend in the future that provides us infinite computing and capability, but still security and privacy is a big challenge for cloud computing.
As we have tried factors on the different types of honeypot algorithm. In the near future we can try this virtualization algorithm on the run time phase, so that we can increase the efficiency and accuracy to makes the data more secure.

REFERENCES

[1]. G. E. Blonder, "Graphical password," U.S. Patent 5 559 961, Sep. 24, 1996.
[2]. Dhamija, et.al, " A user study using images for authentication," in *Proc. 9th USINEX Security Symp., Denver, CO,* Aug. 2000, pp. 45– 58.
[3]. X. Suo,et.al,"Graphical passwords: A survey," in *Proc. 21stAnnu.Comput. Security Appl.Conf.*, Dec. 5–9, 2005, pp. 463–472.
[4]. Paul. A.J, et.al"A Fast and Secure Encryption Algorithm For Message Communication", *IET-UK International Conference on Information and Communication Technology in Electrical Sciences* (ICTES 2007), Dr. M.G.R. University, Chennai, Tamil Nadu, India. pp. 629-634.
[5]. Joshi Ashay Mukundrao, et.al, "Enhancing Security in Cloud Computing" *Information and Knowledge Management* ,ISSN 2224-5758 (Paper) ISSN 2224-896X,Vol 1, No.1, 2011.
[6]. Ajeet Kumar Gautam, et.al, "An Improved Hybrid Intrusion Detection System in Cloud Computing" *International Journal of Computer Applications* (0975 – 8887) Volume 53– No.6, September 2012.
[7]. Stephen Brown,et.al, "Honeypots in the Cloud" *University of Wisconsin – Madison*, December 19, 2012.
[8]. Nithin Chandra, et.al ,"Cloud Security using Honeypot Systems", *International Journal of Scientific & Engineering Research* Volume 3, Issue 3, March -2012 1 ISSN 2229-5518 IJSER © 2012.
[9]. Michael Beham , et.al ,2013, "Intrusion detection and Honey pots in nested virtualization environments", *DSN, 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks* Budapest June 24, 2013 to June 27, 2013 pp1-6.
[10]. Hwan-Seok Yang, "A study on attack information collection using virtualization technology" 74:8791–8799 DOI 10.1007/ s11042-013-1487-8, Springer Science + Business Media New York 2013.
[11]. Al Awadhi, E, et.al,"Assessing the security of the cloud environment" 17-20 Nov. 2013 *IEEE Conference*, Page(s) 251 – 256.
[12]. Kumar Shridhar, et.al, " A Prevention of DDos Attacks in Cloud Using Honeypot" *International Journal of Science and Research (IJSR)* ISSN (Online):2319-7064 Impact Factor(2012): 3.358 Volume 3 Issue11, November , 2014.
[13]. Muhammet Baykara, et.al, "A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems" *International Journal of Computer Networks and Applications (IJCNA)* Volume 2, Issue 5, September – October (2015)
[14]. Ramya. R,"Securing the system using honeypot in cloud computing environment", *International Journal of Multidisciplinary Research and Development* ,Volume: 2, Issue: 4, 172-176 April 2015.
[15]. Sultan Aldossary, et.al, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions" IJACSA) *International Journal of Advanced Computer Science and Applications*, Vol. 7, No. 4, 2016.
[16]. Gagan,et.al, "Dynamic Cluster based Privacy-Preserving Multi-Keyword Search over

Encrypted Cloud Data" *IEEE 2016 6th International Conference - Cloud System and Big Data Engineering* (Confluence) 978-1-4673-8203-8/16/$31.00_c 2016

[17]. Yunfei CI, et.al," Design and Implementation of the Components of the Symmetric Cryptographic Algorithm" *IEEE Second International Conference on Data Science in Cyberspace* 978-1-5386-1600-0/17 $31.00 © 2017 IEEE DOI 10.1109/DSC.2017.23

[18]. Liangxuan Zhang, et.al," Privacy-Preserving Attribute-Based Encryption Supporting Expressive Access Structures"2017 *IEEE Second International Conference on Data Science in Cyberspace* 978-1-5386-1600-0/17 $31.00 © 2017 IEEE DOI 10.1109/ DSC.2017.61

[19]. https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/