A Review on Honeypot Deployment

Dr. Apurva Saxena Verma & Dr. Anubha Dubey

Rabindranath Tagore University

ABSTRACT

A honeypot is a source which is proposed to be attacked and cooperated to gain more information about the attacker and its used tools. It can also be installed to draw and divert an attacker from their existent targets. The honeypots are planned and placed in a cloud network to gather the strange presence as well as known occurrences happened in cloud computing. Honeypots are a computer software tool designed to help, learn the purpose and methods of the hacker community. Honeypot describes in-depth the concepts of their involvement in the field of security. The present review paper proposes and designs the importance of honeypot deployment technique in the protection of data based on the in- frastructures of honeypot, its advantages and disadvantages. The authors also try to offer possible solutions for issues that are generated while using honeypot.

Keywords: honeypots, attacker, information, technique.

Classification: C.2.m

Language: English

London Journals Press

LJP Copyright ID: 975841
Print ISSN: 2514-863X
Online ISSN: 2514-8648

London Journal of Research in Computer Science and Technology

Volume 20 | Issue 1 | Compilation 1.0

A Review on Honeypot Deployment

Dr. Apurva Saxena Verma[α] & Dr.Anubha Dubey[σ]

ABSTRACT

A honeypot is a source which is proposed to be attacked and cooperated to gain more information about the attacker and its used tools. It can also be installed to draw and divert an attacker from their existent targets. The honeypots are planned and placed in a cloud network to gather the strange presence as well as known occurrences happened in cloud computing. Honeypots are a computer software tool designed to help, learn the purpose and methods of the hacker community. Honeypot describes in-depth the concepts of their involvement in the field of security. The present review paper proposes and designs the importance of honeypot deployment technique in the protection of data based on the in-frastructures of honeypot, its advantages and disadvantages. The authors also try to offer possible solutions for issues that are generated while using honeypot.

Keywords: honeypots, attacker, information, technique.

Author α: Research Scholar, Computer Science Engineering, Rabindranath Tagore University, Bhopal, India.
σ: Independent Researcher and analyst, Bioinformatics, MANIT, Bhopal, India.

I. INTRODUCTION

A honeypot is a program, machine, or system that is putting on a network to attract the attackers. The idea is to mislead the intruder by making the honeypot, which seems like a genuine system. Honeypots are naturally virtual machines that follow real machines by simulate running services and open ports, services which one might find on a typical machine on a network. This means, that a honeypot is expected to get attacked and potentially subjugated [2]. Honeypots do not fix anything. A honeypot is a security resource whose importance lies in being surveyed, attacked. In simple terms, “A honeypot is a software system on the Internet that is definitely set up to attract and "trap" people who endeavor to infiltrate other people's computer systems [3].

Maintaining a honeypot is said to require a substantial amount of attention and may propose as its highest value nothing more than a learning experience. The area of computer security, a honeypot is considered to capture all traffic and movement directed to the system. Honeypots differ from regular network systems in that considerably greater emphasis is placed on logging all activity to the site, either by the honeypot itself or through the use of a network/packet sniffer [3]. It is intended to look like something a trespasser can attack to gain contact to a given system. According to the usage honeypots are classified as Production honeypots and Research honeypots.

- Production honeypots are used to diminish the risks in the business/production environment and thus are mostly deployed in organizations [3].
- Research honeypots are intended to congregate as much information as possible. While research honeypots do not append security value to an organization, but they can help a lot in understanding the attacker’s society and their intentions [3].

Every traffic from and to a honeypot is apprehensive because no productive systems positioned on this resource. All data collected by a honeypot is consequently fascinating data. Data

London Journal of Research in Computer Science and Technology

collected by a honeypot is of high assessment and can lead to a better perceptive and acquaintance which in turn can help to amplify overall network security [6]. One can also argue that a honeypot can be used for hindrance because it can discourage attackers from attacking other systems by engaging them lengthy enough and combine their resources. According to their level of involvement, they categorized into three types:

- *Low involvement:* It is the level in which the honeypots imitate simple services, and the freedom given to attackers is least. They are inactive in approach so attackers cannot use them to attack other systems. Thus they are well suitable for organizations, and many production honeypots are low involvement honeypots.
- *Mid involvement:* This honeypot grants more services than low level but doesn't provide a real operating system [3]. The risks also rise with the level of emulation they provide to attackers.
- High involvement: This honeypot gives an excellent operating system to attack. Expose the system to sufficient risk and complexity. At the same time, the possibility to build up information about the attack as well as the magnetism of the honeypot increases a lot, so they primarily used for research purposes.

Figure 1 shows all levels of honeypot at a glance, types of a honeypot, their deployment mode which further categorized into three different ways. Legal and ethical issues are also tried to incorporate with the architecture.

Contribution of authors: In this review paper authors are trying to compile working of different honeypots. Besides advantages and disadvantages, an effort is trying to design a proposed solutions for issues obtained during applying honeypot. And ethics of using honeypot in cloud are also discussed.

Paper organization: The remainder of this paper is organized as follows. Related works are summarized in Section II. The advantages of honeypot are explained in Section III. In section IV the detail description of drawbacks of honeypot and its issues with proposed solutions. The significance of honeypot in various fields is describes in the section V. Ethics of Honeypot is explained in section VI. Finally, we conclude the paper with its future scope in Section VII.

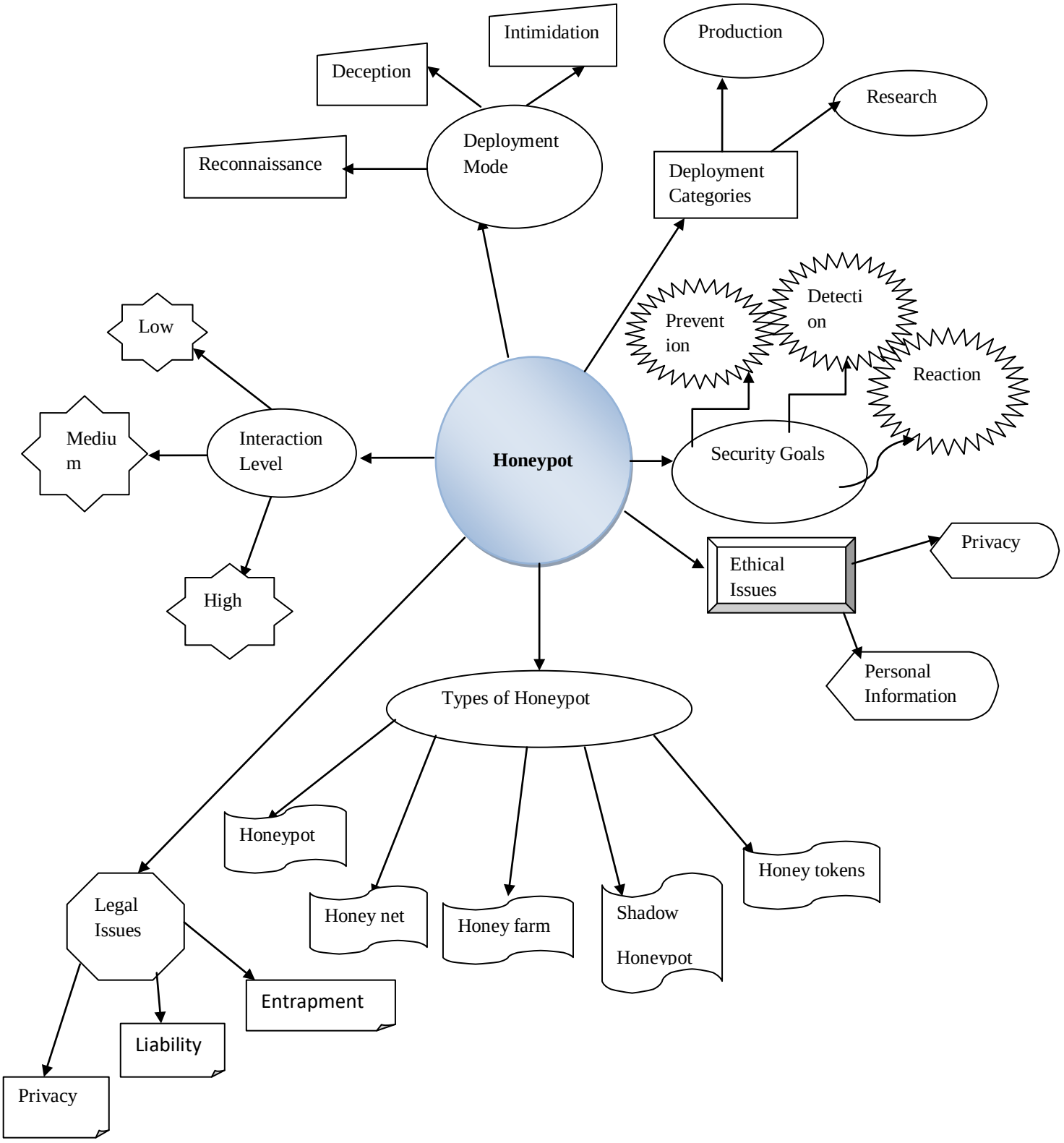

Figure1. Honeypot architecture

II. RELATED WORK

Paul. A.J, et al. 2007 presented security in a cloud computing environment mostly uses this infrastructure as a service for the research work. They provide opportunities for offering capital cost and focused on core competencies. The purpose of this paper is to use Honey pot as a security tool in a cloud environment.

Joshi Ashay Mukundrao et al. 2011 discussed cloud computing is the newly emerging field because of its performance, high availability, least cost. In cloud computing, the data get stored in service providers. This paper has been written to focus on the problem of data security.

Stephen Brown et al. 2012 conducted a study using honeypots within various cloud computing platforms such as Amazon EC2, Windows Azure etc. to learn more about what kind of packets they receive. They used multiple honeypots such as Dionaea, Kippo, and Amun on the cloud instances. They gathered data about where attacks came from, what kinds of attacks made, and various cloud instances.

Nithin Chandra et.al, 2012 presented a Cloud Security using Honey pots. The concepts were first introduced by several icons in computer security, specifically Cliff Stoll in the book “The Cuckoo's Egg”, and Bill Cheswick's paper “An Evening with Berferd." This paper explained that honeypots are used for securing cloud systems, their advantages and disadvantages etc.

Michael Beham et.al, 2013 explained that in many organizations reasonably attractive towards the services which are used in a cloud environment. This study of the security in the cloud environment is assessed by deploying and running Dionaea honeypots for a few months in the cloud provide networks.

Hwan-Seok Yang, 2013 explained that in cloud computing, intrusion detection and prevention systems are one such measure to lessen the attacks. Different researchers have proposed different IDSs time to time. Some of these IDS’s combine features of two or more IDSs which are called as hybrid intrusion detection Systems. For a signature based IDS if an attacker attacks slowly and organized, the attack may go undetected through the IDS. Thus, signature-based IDS fail to detect unknown attacks. Hybrid Intrusion Detection System (HIDS) combines the positive features of two different detection methodologies -Honeypot methodology and anomaly based intrusion detection methodology.

Navneet Kambow et.al, 2014 said that network forensics is used to notice attacker’s activity and analyze their behavior. This assessment paper is based upon the preface to honeypots, their significance in network security, types of honeypots, their advantages, disadvantages and legal issues connected to honeypots.

Huseyin Ulusoy,et.al 2015 gave many research projects from the past, and built intrusion detection systems and honeypot architectures based on virtual machine introspection (VMI). These systems directly provide benefit from the use of virtualization technology. They compare the performance of existing nested-virtualization solutions and analyze the impact of the performance overhead on VMI-based intrusion detection and honey pot systems.

Ramya. R, cloud 2015 explained in cloud computing, accessing the data from data centers reduces the chances of eavesdropping and storage cost. A honey pot is a system that intentionally designs to invite malicious users to enter in the network. Honeypots is used in various cloud computing platforms (such as Amazon EC2, Windows Azure etc.) with the objective of learning more about what kind of packets they receive. Malicious activities of the attacker are used to educate the network from the attack and design network with the novel security tools.

Chaimae Saadi et.al 2016 explained that cloud computing security has developed into a basic necessity. It attains knowledge about vulnerabilities, attacks, activities of attackers and

tools to secure it. This work suggests new cloud infrastructure architecture, which combines IDS based on mobile agent and using three types of honeypots in order to detect attacks, to study the behavior of attackers, augment the added value of Honeypot and IDS based mobile agents, to solve systems boundaries intrusion detection, recover knowledge bases IDS. Therefore boost the detection pace in the cloud environment.

Manoj Agnihotri 2017 has explained that cloud computing provide contact to large pools of high end resources through diversity of interfaces that are comparable to the move toward in HPC computing resource management. The honeypots are planned and placed in a cloud network that help us to collect the unknown as well as recognized incidents occurred in cloud computing. The purpose of this paper is to show the significance of honeypot in the protection of cloud based infrastructures.

Michail Tsikerdekis et.al, 2018 explained that honeypots has been used lengthily for over two decades. They also provide recommendations for future honeypot software which is more flexible, modular and include a dynamic intelligence design.

Christos Dalamagkas et. al, 2019 compared honeypot with the smart grid technology to distract the attackers interest and investigate the intruder strategies to protect the real data. Conpot as honeypot used to support many smart grid cases was also shown.

III. WORKING OF HONEYPOT

Authors are tried to compile the different honeypots and their working in the different environment of operating system in table 1. These involve different interaction level of honeypots, their log files generated, services, and their requirements on the basis of available literature [3].

Table 1: Compare among Various Honeypots.

Honeypots	Interaction Level	Types of Honeypot	Software Type	Log Files	Services	OS	Requirements
BOF(Back Office Friendly)	Low Interaction Level	--	Freeware	NO	7 (Telnet,FTP,HTTP, POP3,imap2)	Win32,Unix	--
Specter(Spec 03)	High Interaction Level	Production Honeypot	Retail Software	YES	14 (SMTP,FTP,POP3, HTTP,SSH,DNSim ap4,Telnet)	WindowsNT ,2000,XP	--
Decoy Server (Deco02)	High Interaction Level	--	NO	Syslog	Unlimited	Windows (9X,2000,N T),Solaris	Java Runtime
Honeyd(prov03)	Medium Interaction Level	--	YES	YES	Unlimited	Unix	Libdnet, Libevent
KF Sensor	Medium Interaction Level	Production Honeypot	NO	NO	Unlimited	Win32	HTTP
Dionea	Medium Interaction Level	Production Honeypot	YES	YES	FTP,HTTP,MYSQL	Ubuntu	--

IV. ADVANTAGES OF HONEYPOTS

Honeypots have several advantages exclusive to technology. Most notable are explained here [11].

- *Data rate:* The complete quantity of information is irresistible, building it enormously complicated to obtain some value from the data. Honeypots can give us the accurate data we needed in a rapid and easy-to-recognize design. This makes the study easier and response time is much faster.

- *Resources:* One more challenge for the security mechanisms is its limitations. But honeypot does not need the newest cutting-edge technology and vast amounts of RAM. In minimal number of computers it deploys easily and performs better. This means honeypot is relatively cheaper in terms of availing the resources [11].
- *Accessibility:* The researchers believe in simplicity, is the prime advantage of honeypots. Here no algorithms to develop and no databases to sustain. Whereas some honeypots, particularly research honeypots, are involved on the basic principle.
- *Return on the stake:* As firewalls fruitfully remain intruders away, they turn into sufferers of their accomplishment. Administration start inquiry about the return on deal, by differentiating a threat gets disappear: Investments has new protection technologies, such as robust validation, encryption, etc.
- *Reduced False Positives:* Honeypots help in dipping false positives. The better the probability that a security resource produce false positives or misleading alerts, the fewer likely the technology will be installed [19].
- *Catching False negatives:* Catching false negatives with the help of honeypots is calm comfortable because every connection made to a honeypot is considered unauthorized. Conventional attacks detecting tools become failing in detecting new attacks like signature- based detection tools [18].
- *Encryption:* Honeypots can detain malicious activity if it is in an encrypted form.

V. DRAWBACKS OF HONEYPOTS

Amid amazing recompense, honeypot consists of numerous obstacles because they work with security mechanism and enhance the overall architecture of security.

- *Narrow Field of outlook:* They observe activity against the intruder [8]. An invader splits the network and attacks on systems.
- *Fingerprinting:* In this technique, an attacker identifies the accurate uniqueness of a honeypot as it contains exceptionality [9].
- *Risk:* They launch threat in our surroundings. Several honeypots have unique levels of risk. Low interaction honeypots has low chances, but high interaction honeypots introduce high risks in whole possible platform for the attacker. The simpler the honeypot, minor will be a risk.

VI. HONEYPOT: ISSUES AND PROPOSED SOLUTIONS

There are some issues generated while using honeypot, which is tried to solve through the proposed possible solutions are given in table2.

Table2: Honeypot on different OS, its issues and proposed possible Solutions

Honeypot	Linux	Windows	Issues	Possible Solution
Open Source	NO	NO	This tool is Simulate	➢ Used in Virtual environment with proper Security facility
Services	Web Server(HTTP,FTP,SSH)	IIS,FTP	Easy to Deploy	➢ Honeypot can be used in cloud environment where security gets enhanced. ➢ Alert system generated ➢ Log files can be formed ➢ Continuous system monitoring possible.
Database	MYSQL	MYSQL	On real System	➢ Security get increased on cloud environment ➢ Another tool can be added like Kerberos which increases the security. ➢ Here risk gets decreases and chances of gathering information about attacker get increases.

Modifying Syslog	Syslogd, Klogd	-		--
Logging	Bash or Script Session	Perl Script, PHP Scripts		--
Port No.	8080	8080		--
Integrity Checking	Tripwire	-		--

The flaws can be removed [22] if the above solutions are used as per requirement. It is also tried to explain the working of honeypot on the different operating system.

VII. SIGNIFICANCE OF HONEYPOT

- *Honeypots in Educational Resource:* Jeremiah K. Jones & Gordon W. Romney [3] discussed the aspects of using the honeynets in an educational area. A lab of honeypot can form for tracing the malicious traffic in the network[22].The honeypot is implemented at Brigham Young University observe the certain benefits such as it inform about the new threats, securing the lab at a higher level, learning the network, basics of security closely identifies the flaws.
- *Virtual Honeynet in Teaching and Research:* An additional way of implementing the honeypot in the educational areas can be done by executing real or virtual honeynet for better understanding [23]. In the real honeynets, all the connections have to be measured very generously to eliminate any possibility of fault.
- *Honeypot with IDS:* An Intrusion Detection System (IDS) distinguishes between the traffic coming from various customers and the attackers, to concurrently ease the problems of throughput, latency and security of the Network. IDS can be further categorizes into Network based and Host-based [24]. Honeypots can either be the host and Network based, but generally, they are not network-based as all interface operations characteristically performed over a network link.
- *Honeypot uses in cyber security:* Honeypot can be used in Cyber security to stop the malicious attack from the attacker. Deception technology is a future concept of cyber security defense. Its related application can detect, analyze, and defend against minimal time period and advanced attacks in real time [24]. As a technique honeypot can be attach with different technologies to empower the security on the basis of the some examples of honeypot such as Spam honeypot. It is used to attract spam and unauthorized emails, malware honeypot is designed as a simulator to get the malware attacks, spider honeypot is designed as a false web-page to detect and analyze on the basis of the unusual activity and many more.
- *IoT (Internet of Things) with honeypots:* The Internet of things is defined as the series of multiple technologies, real-time analytic, machine learning, commodity sensors, and embedded systems. The Honeypot tool that is mostly using in IOT is:
- *Honey Thing:* This honeypot act as a modem or router run on the web server and support TR-069(Technical Report 069) protocol [23]. It offers an easy web-based interface.
- *Database honeypots:* It is designed to find different attacking techniques through SQL (Structured Query Language) service. One of the tools given below:
- *Elastic Honey:* This honeypot is created for database which catches the malicious request from the attacker.
- *Honeypot with Cloud provider:* To enhance the security of the data with the cloud services we can append the honeypot with it. There are several honeypot available which can be used as per the need [25].
- *Honeypot with Kerberos:* It can also be attached with the tools or software like Kerberos to increase the security and make the data continuous monitoring from the attacker [26].

VIII. ETHICS OF HONEYPOT

Cloud computing brings so many profits to organizations that are mostly unfeasible to resist migrating to it [22]. The Cloud has transformed the business but also has quickly turned into a hacking quicksand, who miscalculates the power and importance of proper cloud security. Various technical criteria have authority on arising of ethical issues in Cloud. Along with them, security, privacy, compliance and performance metrics have a better impact on moral matters.

Subsequently, we tried to demonstrate how each of these technological criteria can have a direct impact on ethical considerations in Cloud:

a) Privacy and Security: When illegal access to your responsive data tenant in a Cloud is gained, either by a hacker or by the Cloud provider itself. Hence privacy and security mechanisms are essential to avoid such ethical issues.
b) Compliance: A significant part of privacy and security mechanisms created as a set of principles. A cloud service should obey with a subset of the standards concerning the request of the service. When a Cloud-based appliance in the SaaS model with some privacy or security necessities is going to be launched in the market, it should fulfill the predefined standards [23]. Additionally, it is one of the critical parameters to choose a cloud supplier to get either IaaS or PaaS services.
c) Performance metrics: The expected performances of the provided services are predetermined in Service Level Agreement (SLA), which is a part of the general terms and conditions, focused on the performance metrics [22-23]. Availability and application response time is a pair of examples of SLA metrics. The violation of the performance metrics of SLA is a punishable offence.
d) Security is the primary factor preventing organizations from migrating to the cloud. With the central security pressure like unauthorized access, hijacking, and malevolent insiders. The first step is to intensify cloud security consciousness among staff to diminish the human factor in security occurrences.

IX CONCLUSION AND FUTURE SCOPE

A honeypot is a valuable resource, mainly to assemble information about events of attackers as well as their deployed tools. However, there have been numerous research offerings to make honeypot technologies more secure, reliable and risk-free.

In this paper, we have given an overview of the classification of honeypots technologies with their advantages and disadvantages. We recommended the use of an appropriate kind of honeypots for certain specific applications which depends on the interaction and design of the system. In the future we can try to find out possible solution of syslog, logging, integrity checking. By the use of deception technology examples, the level of security will get enhanced and made the honeypot much more than the software tool for research. This technology makes the honeypot more advanced at the level of authenticity, ease to operate, interactive, scalable in physical, virtual and cloud environment. Flexible deployment is one of the properties of the deception technology which is used in machine learning.

A combination of traditional network security monitoring and recent advancements in honeypots would be like:

- Cloud environment: In the cloud, honeypot can be effective tool for information gathering.
- Grid computing: It is used to secure high interaction honeypot by secure protection language (SPL).SPL to enforce security properties which cannot manage with other approach.
- Edge computing: Here honeypot can be used as active cyber defense techniques of a specific organization.

REFERENCES

1. Dhamija, et.al, " A user study using images for authentication," in Proc. 9th USINEX Security Symp., Denver, CO, Aug. 2000, pp. 45– 58.
2. Reto Baumann et.al 2002 White Paper: Honeypots .
3. Fabien Pouget, Marc Dacier et.al, 2003 White Paper: "Honeypot, Honeynet, Honeytoken: Terminological issues1 Institute Eurécom 2229, Route des Crêtes ; BP 193 06904 Sophia Antipolis Cedex ; France.
4. X. Suo,et.al,"Graphical passwords: A survey," in Proc. 21stAnnu.Comput. Security Appl.Conf., Dec. 5–9, 2005, pp. 463–472.
5. Paul. A.J, et.al 2007 "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.
6. 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.
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 pp 1-6.
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. Navneet Kambow et.al 2014 Honeypots: The Need of Network Security (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6098-6101.
12. 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.
13. Chaimae Saadi et.al, 2016 Cloud Computing Security Using IDS-AM-Clust, Honeyd, Honeywall and Honeycomb International Conference on Computational Modeling and Security (CMS 2016) doi: 10.1016/ j.procs. 2016.05.189
14. 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.
15. 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
16. 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.
17. Manoj Agnihotri et.al 2017 Analysis of Cloud Security through Honeypots International Journal of Innovations in Engineering and Technology (IJIET) http://dx.doi.org/10.21172/ijiet. 82.034.
18. Nooreen Fatima Khan et.al 2018, Cloud security using self-acting spontaneous honeypots International Journal of Engineering & Technology 7 (2.8) (2018) 243-247
19. Michail Tsikerdekis et.al, 2018 Approaches for Preventing Honeypot Detection and Compromise 978-1-5386-5150-6/18/$31.00 © 2018 IEEE.

20. Ronald Mitchell Campbell, 2013 The legal and ethical issues of deploying Honeypots Honor .project University of South Africa.
21. Fahien Pouget et.al, 2003 Whitepapers: Honeypot, Honey net: A Comparative Survey, Eurecom issues September14 2003, France.
22. Aman Sachan, et.al, 2016 Honeypots: Sweet OR Sour spot in Network Security? International Journal of Current Engineering and Technology Vol.6, No.3 (June 2016).
23. Yogendra Kumar Jain et.al, 2011 Honeypot based Secure Network System, International Journal on Computer Science and Engineering (IJCSE) Vol. 3 No. 2 Feb 2011 ISSN : 0975-339.
24. Christos Dalamagkas, et. al, 2019"A Survey On Honeypots, Honeynets And Their Applications On Smart Grid" IEEE NetSoft 2019 - 1st Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-Defined and Virtualized Infrastru- ctures (SecSoft).
25. Apurva Saxena, et.al, 2019 Kerberos based Data security in Research & Production Honey Pot. EPH - International Journal of Science and Engineering Volume-5, Issue-1, Jan.
26. Apurva Saxena, et.al,2019 "KERBEROS AUTHENTICATION MODEL FOR DATA SECURITY IN CLOUD COMPUTING USING HONEY-POT" GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES [Saxena, 6(8): August 2019] ISSN 2348 – 8034 DOI- 10.5281/zenodo. 3367428.