JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

AN ENHANCED INTRUSION DETECTION AND PREVENTION SYSTEM FOR CLOUD STORAGE USING HONEYPOT

[1]Chavan Smita Bajirao, Student, Department of Computer Science, MVJ College of Engineering, Bangalore, India

[2] Dr. Sudhan M B, Associate Professor, Department of AI and ML, MVJ College of Engineering, Bangalore, India

Abstract: Most associations are currently moving their administrations into the cloud to offer a more adaptable, open, portable and pervasive help. In any case, this additionally carries more openness to security dangers, digital assaults and challenges in unwavering quality and wellbeing. The proposed plan is to send a Honeypot in the Intrusion Detection and Prevention System (IDPS) model to ensure improved execution, extended degree of safety in the Cloud processing climate and decrease in the threats to the Cloud climate - by zeroing in on the issue of how the data is put away in the Cloud. The proposed structure is feasible and the model successful, concerning use of the planned IDPS and Honeypot by an association. The structure depicted utilizes both Anomaly Detection (AD) and Signature Detection (SD) in joint effort, to recognize various assaults and deny them access through the utilization of the proposed Intrusion Prevention System (IPS). The goal of this report is to feature, perceive and ensnare inward interlopers by the utilization of the Honeypot.

Key words: IP networks, Tools, Computer hacking, Firewalls (computing), Intrusion detection, Cloud computing.

1. INTRODUCTION

Honeypots are expected to distinguish, gather, and forestall assaults. They produce early alerts of possible dangers and assaults. Honeypots are not difficult to set up and record the essential data. Companies principally use them to shield their frameworks from interlopers. Honeypots are implanted in firewall programming. Accordingly, they are more reasonable. A honeypot is a security resource with a not set in stone by its capacity to be analyzed, went after, or exchanged. Rather than being utilized for evasion, the honeypot is utilized for reaction and location.

Honeypots don't recognize explicit interruptions or infections; all things considered, they gather information and distinguish the assault design. Protectors can then answer this affirmation by sustaining their safeguard and countermeasures against future security dangers. The honeypot fills in as a checking and cautioning framework. It is an organization or framework site that gives off an impression of being a different framework part. For of entanglement, it is deliberately intended to contain information that is critical to developers and programmers.

Inside gatecrashers are more normal than outer assailants. Thus, the best way to safeguard against inward gatecrashers is to send a honeypot behind a firewall in IDPS on a Cloud Computing Environment, which is likewise the framework proposed in this task. A straightforward IDPS might involve port checking in the Cloud Computing Environment.

2. PROBLEM STATEMENT

Numerous organizations are as of now moving their PC administrations to the Cloud. This significantly further develops how effectively shoppers can get to their PC handling. Notwithstanding, it additionally conveys with it pristine security dangers and unwavering quality related challenges.

Since it offers versatile deals for suppliers and openness and constancy choices for clients, distributed computing is really an alluring and cost-saving answer for clients. Albeit engaging, cloud innovation presents various new security dangers and challenges with regards to introducing IDS in cloud conditions.

Most of IDSs are made to manage specific sorts of dangers. Clearly nobody technique can give affirmation against future dangers. As a result, there is a need for an integrated plan that can offer effective defense against the whole spectrum of threats.

3. LITERATURE SURVEY

Iglesias, (2020) [1], the Honeypot can be utilized for learning about the assaults in a specific framework or in an overall climate relying upon the requirements. Subsequently Honeypot go about as a perfect source place for learning the strategies about the data and execution plan of programmers. Other organization checking gadgets like Intrusion Detection System (IDS) chiefly center around dissecting the examples for recognizing the malevolent traffic assets. However, they exacerbate a befuddle in design revamping so they lead to large number of bogus positive and negatives. While in Honeypot all bundles are treated as dubious, so they become simpler in arranging the vindictive records. The data's are gathered in light of the login highlights which are having the remarkable data about the log history, which typically don't win in different frameworks like IDS. Despite the fact that the encryption of organization traffic.

Another significant element existing in the Honeypot is that they persevere through even in recognizing the new pernicious records which is being selected. This component isn't upheld by IDS as they predominantly support the mark-based design acknowledgment. Honeypot is the characterized PC to draw in the aggressors for investigating the thoughts of assailants. Honeypot are simply intended to mirror like a genuine PC where they claim to help the gatecrasher in breaking the genuine framework. The engineering of a Honeypot is planned so that it upholds as a wellspring of collaboration for interfacing with a dark feline local area.

They are planned so that they set to identify neutralize made for the entrance of unapproved data. At first genuine part is set which are as information. They are planned extraordinarily, so they set to recognize check made for the entrance of unapproved data. At first real part is set which are in type of information. They are typically disengaged while checking and gathering data, then they are obstructed.

To match the recent fads in the organization and their plan measures new Honeypot have been planned. Barrenoet al. (2020) Hybrid model has been proposed where the connection between the low-collaboration and high communication half and half Honeypot is made to acquire the reaction. The fundamental arrangement depended on the intermediary present in each host. They empower utilizing the virtual hosts alongside rescheduling of organization traffic. Jin et al. (2020) the observing of a Honeypot is empowered without making the malware to get away from the framework. This aides in getting the detail data about the assailants and furthermore made the Honeypot to be separated from the aggressors in recognizing them. Krawetz (2020) the honey product was created to find the vindictive web and URL [2].

This was figured out to be opportunity consuming one in the identification and the examination showed that the nitration among high and low connection Honeypot is fundamental. Broadway et al (2020) completed a trial and error to decrease the bogus positive and negative rate. To draw out the arrangement shadow Honeypot were made. They duplicated the approaching solicitations in the shadow Honeypot servers so it executes like the creation server. The implanted Honeypot codes were sent in them for observing the way of behaving. The strategy includes in the handling of approaching solicitation utilizing irregularity recognition method, this brought about high bogus up-sides caution. Camastraet al (2020) shows the incorporation of low and high-collaboration Honeypot was made to bring the answer for deciding the width of Honeypot inclusion. Chang et al (2020) expressed the technique for disengaging the creation server and concealing them was proposed to diminish the refusal of-administration assault [3].

Overall Honeypot don't confirm the client, where as in the proposed technique the dynamic server was introduced to validate the client. This guarantees the framework to be away from DoS assault. Chenet al (2020) shows the significance of making security to the switches was proposed. They made the client-side Honeypot to decide the assailants hacking the switches. For this Quagga apparatus was utilized for breaking down the action of the switch. Wireshark was utilized to track down the reaction from the switch movement. Chenet al (2020) introduced an original sensor-based screen high-collaboration Honeypot The sensor set inside the module assist in assessing the vindictive movement and data about the framework with calling. Different sensors are utilized to screen the traffic. Hoque, Net al (2020) expressed how to limit the 33 disavowal of administration assault rearranging of Honeypot and creation servers was made. Honeypot were made to trap the assault to diminished DoS assaults. Cheng et al (2020) asserted about signature age for interruption discoveries were found to dispose of the multi day assault. Dressler guaranteed that the Honeypots were intended to screen the action of phishers. Faghani proposed a clever Honeypot to recognize worm proliferation. Levine, (2020) proposed a clever online Honeynet to safeguard venture organizations. The key thought is to involve the web clawers for surface enormous number of web servers for consequently recognizing malevolent web servers. Argos based Honeypot guaranteed the dialing back the action of obscure malware. This is finished by powerfully embedding shell code to get data about assailant thus to make them to execute boundless circle for limiting the damage. Iglesiaset al (2020) expressed about the plan of sham Honeypots to oppose assailants. The key thought expressed by the creator about Honeypot procedure is to consequently distinguish the malware, and catching it by making correlation with marks like MD5 hashes [4].

Lai-Ming Shiue et al, (2021); The Honeypot doesn't connect with direct admittance to supporting the required of the association. So, they are intended for examining the dangers so that it's simpler for the sending and investigation of dangers against the security. However, the Honeypot include in convoluted arrangement, are broadly liked as they are utilized for catching the touchy data, that can be utilized in the security reason for military and other government association [5].

4. PROPSED METHODLOGY

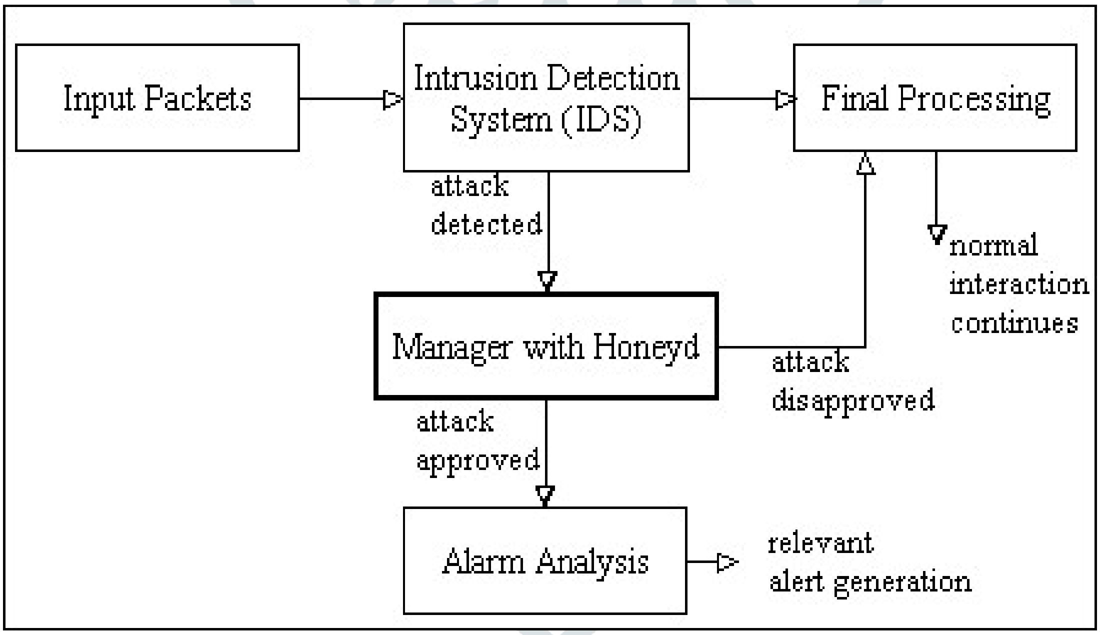

FIG 1: PROPOSED METHODOLOGY

Honeypots are intended to recognize, accumulate data, and forestall assaults. They produce danger and assault early admonition signs. Honeypots are easy to utilize and monitor vital information. They are fundamentally utilized by partnerships to shield their frameworks from gatecrashers. Honeypots are concealed inside firewall software engineers. Accordingly, they can be better made due. A honeypot is a kind of safety resource who's not entirely set in stone by its capacity to be examined, went after, or exchanged.

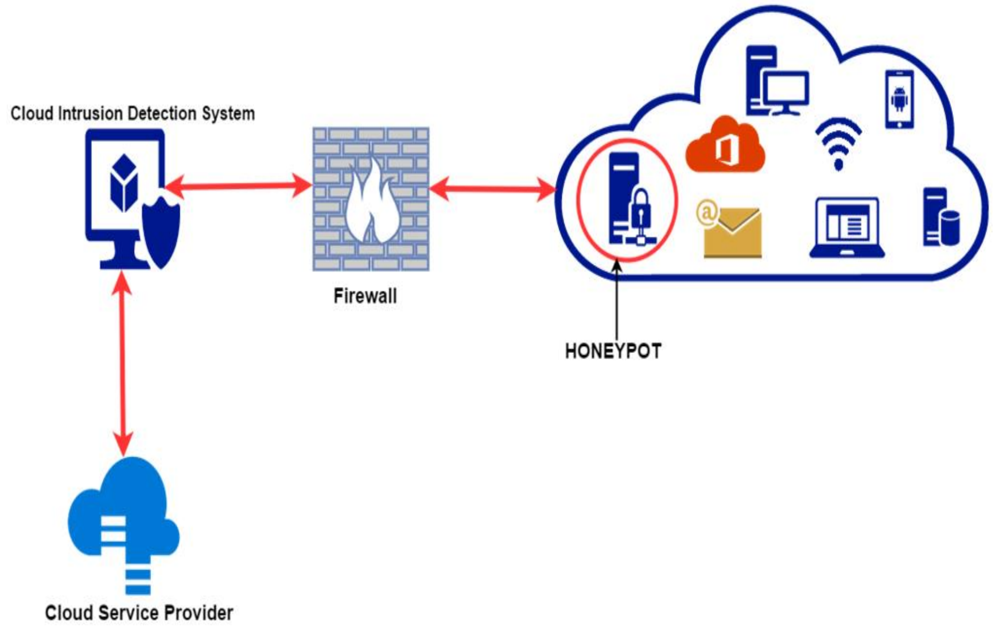

FIG 2: PROPOSED METHODOLOGY

This proposes that whatever is assigned as a honeypot exists exclusively to test, assault, and possibly abuse the framework. The honeypot is utilized for reaction and recognition as opposed to aversion. Honeypots don't distinguish specific interruptions or infections; all things considered, they gather information and recognize the assault procedure. Protectors are prepared to do then, at that point, answer this affirmation by invigorating their guard and defends against future security dangers.

```
Algorithm

I    IDS Algorithm

STEP 1: Read incoming data from users

STEP 2: IF Data size is in limit:

        Forward data to Server

        ELSE

        Consider as suspicious activity

STEP 3: Repeat step 2 until suspicious data received 3 times

STEP 4: Update suspicious user details in honeypot

II   HONEYPOT ALGORITHM

STEP 1: Read suspicious user details

STEP 2: Send validation code to user

STEP 3: Read Validation code and other data from user

STEP 4: IF details matched

        Consider user as genuine.

        ELSE
```

Consider user as attacker and block him

The honeypot fills in as an observing as well as early advance notice framework. An organization or framework area gives off an impression of being a different part of the framework. It is intentionally intended to store incredibly delicate information vital to software engineers and programmers as a type of entanglement. The pace of inner interlopers is really more prominent than the pace of outer assaults. To shield against inner gatecrashers, the main way is to set up a honeypot in the IDPS on a distributed computing climate, which is put behind the firewall.

5. RESULTS

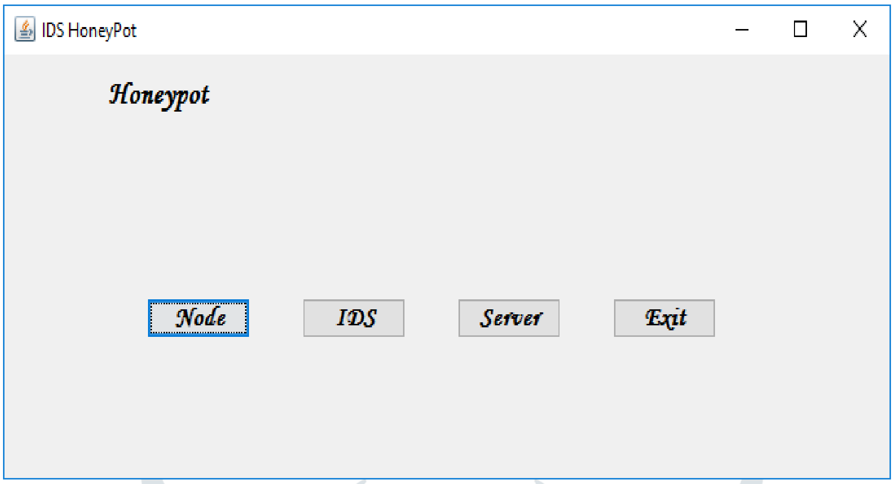

Fig 3. Honeypot Main Screen

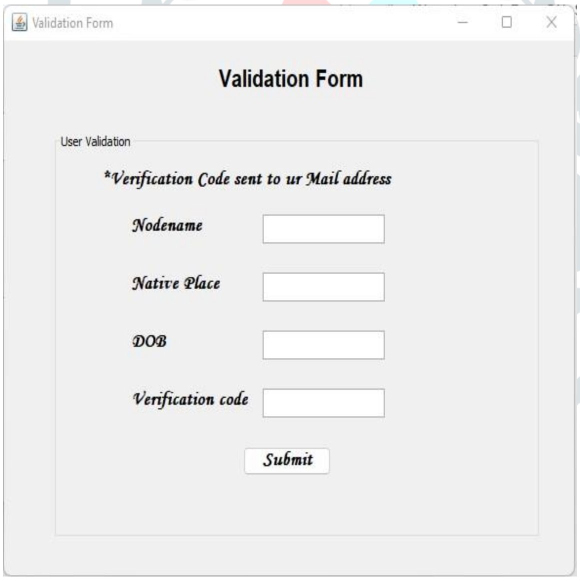

Fig 4. Validation Form

The above figure shows the example plan of the wellspring end planned. The client have different pushbuttons to choose from the rundown to do the different activities. In the principal window have the choice to choose the Node, IDS, Server and exit. The second UI shows the approval structure to be filled prior to presenting the solicitation.

6. CONCLUSION

Honeypots offer new viewpoint on the productivity of such an essential security identification procedure. The log record can be inspected to look further into the starting points of the organization assault as well as other significant subtleties. The honeypot can reenact the main assault, and the recorded occasion can be over and over played back to analyze the assault's procedural strides in more detail.

7. FUTURE SCOPE

More work ought to be placed into creating honeypots later on so they can oversee monstrous measures of traffic information, be impervious to against legal sciences procedures, and broaden the assortment of IoT gadgets that can be imitated.

REFERENCES

[1] Almotairi, S, Clark, A, Mohay, G & Zimmermann, J 2008, ‘Characterization of attackers' activities in honeypot traffic using principal component analysis’, Proc. IFIP Int. Conf. Network and Parallel Computing, pp. 147-154.

[2] Alserhani F, et al., 2009, ‘Evaluating intrusion detection systems in high speed networks’, Proc. 5th. Int. Conf. Inf. Assurance Security, Vol. 02, pp. 454-459.

[3] Baecher, P 2006, ‘The Nepenthes Platform: An Efficient Approach to Collect Malware’, Proc. 9th Recent Advances in Intrusion Detection Conf, pp. 165-184.

[4] Baecher, P, Koetter, M, Dornseif, M & Freiling, F 2006, ‘The nepenthes platform: An efficient approach to collect malware’, Proc. Symp. Recent Advances in Intrusion Detection (RAID'06), pp. 165-184.

[5] Barreno, M, Nelson, B, Sears, R, Joseph, AD & Tygar, JD 2006, ‘Can machine learning be secure? In ASIACCS ’06: Proceedings of the 2006 ACM Symposium on Information, computer and communications security, New York, NY, USA, ACM Press, pp. 16-25.

[6] Bhat, VH 2010, ‘A Novel Data Generation Approach for Digital Forensic Application in Data Mining’, Proc. 2nd Int'l Conf. on Machine Learning and Computing (ICMLC 10), pp. 86-90.

[7] Broadway, J, Turnbull, B & Slay, J 2008, ‘Improving the Analysis of Lawfully Intercepted Network Packet Data Captured for Forensic Analysis’, Proc. 3rd Int'l Conf. Availability Reliability and Security ARES 08, pp. 1361-1368.

[8] Camastra, F, Ciaramella, A & Staiano, A 2011, ‘Machine Learning and Soft Computing for ICT Security: An Overview of Current Trends’, J.Ambient Intelligence and Humanized Computing.

[9] Chang, JC, Yi-Lang & Tsai 2010, ‘Design of virtual Honeynet collaboration system in existing security research networks’ ,Communications and Information Technologies (ISCIT), International Symposium on, pp. 798-803.133

[10] Chen, Chia-Mei, Cheng, Sheng-Tzong & Zeng, Ruei-Yu 2012, ‘A proactive approach to intrusion detection and malware collection’, Security and Communication Networks. pp. N/A.