iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VII **Month of publication:** July 2022

DOI: https://doi.org/10.22214/ijraset.2022.45091

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

Intrusion Detection and Prevention Using Honeypot Network for Cloud Security

N. Shivathmika[1], A. Divya[2], K. Aadi Lakshmi[3], Mr. L. Manikandan[4]
[1, 2, 3]*Undergraduate Student, Department of Computer Science & Engineering, Sridevi Women's Engineering College, Hyderabad, Telangana*
[4]*Assistant Professor, Department of Computer Science & Engineering, Sridevi Women's Engineering College, Hyderabad, Telangana*

Abstract: ***The rapid increase in the number of users, there is a rise in issues related to hardware failure, web hosting, space and memory allocation of data, which is directly or indirectly leading to the loss of data. With the objective of providing services that are reliable, fast and low in cost, we turn to cloud-computing practices. With a tremendous development in this technology, there is ever increasing chance of its security being compromised by malicious users. A way to divert malicious traffic away from systems is by using Honeypot. It is a colossal strategy that has shown signs of improvement in security of systems. Keeping in mind the various legal issues one may face while deploying Honeypot on third-party cloud vendor servers, the concept of Honeypot is implemented in a file-sharing application which is deployed on cloud server. This paper discusses the detection attacks in a cloud-based environment as well as the use of Honeypot for its security, thereby proposing a new technique to do the same.***

Keywords: Honeypot server algorithm.

I. INTRODUCTION

An intrusion detection system (IDS) is software specifically built to monitor network traffic and discover irregularities. Unwarranted or unexplained network changes could indicate malicious activity at any stage, whether it be the beginnings of an attack or a full-blown breach. There are two main kinds of intrusion detection system (IDS): A network intrusion detection system (NIDS) enacts intrusion detection across your entire network, using all packet metadata and contents to determine threats. A host-based intrusion detection system (HIDS) enacts intrusion detection through a particular endpoint, and monitors network traffic and system logs to and from a particular device. The best intrusion detection systems are built to collect network traffic from all devices via NIDS and HIDS, thus increasing the chances of intrusion detection across your IT infrastructure. Honeypots can be defined as systems or assets which are used to not only trap, monitor but to also identify erroneous requests present within a network. They vary in the interaction provided to the attackers, from low interaction to medium and high, each type has its advantages and disadvantages. Their aim is to analyze, understand, watch and track attacker's behavior in order to create systems that are not only secure but can also handle such traffic. It is a closely monitored computing resource that we want to be probed, attacked, or compromised. "More precisely, it is an information system resource whose value lies in unauthorized or illicit use of that resource."

At last, they can essentially sit and log all movement coming into the cloud site; and in light of the fact that it's utilized for this particular reason practically any action ought to be dealt with as instantly suspicious. Honeypots can serve to make dangers more obvious and go about as an early alert framework, which gives a cloud organization a more proactive way to deal with security instead of responsive. Any association with either outside resources/areas or cloud administrations ought to deploy cloud-based Honeypots.

II. RELATED STUDY

Cloud computing has been envisioned as the next-generation architecture of IT enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, 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 article, 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, we propose an effective and flexible distributed scheme with two salient features,

opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server (s).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

A. Software Requirements

The functional requirements or the overall description documents include the product perspective and features, operating system and operating environment, graphics requirements, design constraints and user documentation.
The appropriation of requirements and implementation constraints gives the general overview of the project in regards to what the areas of strength and deficit are and how to tackle them.

- Python idel 3.7 version (or)
- Anaconda 3.7 (or)
- Jupiter (or)
- Google colab

B. Hardware Requirements

Minimum hardware requirements are very dependent on the particular software being developed by a given Enthought Python / Canopy / VS Code user. Applications that need to store large arrays/objects in memory will require more RAM, whereas applications that need to perform numerous calculations or tasks more quickly will require a faster processor.

- Operating system: windows, Linux
- Processor: minimum intel i3
- Ram: minimum 4 gb
- Hard disk: minimum 250gb

A way to divert malicious traffic away from systems is by using Honeypot. It is a colossal strategy that has shown signs of improvement in security of systems. Keeping in mind the various legal issues one may face while deploying Honeypot on third-party cloud vendor servers, the concept of Honeypot is implemented in a file-sharing application which is deployed on cloud server. This paper discusses the detection attacks in a cloud-based environment as well as the use of Honeypot for its security, thereby proposing a new technique to do the same.

C. Existing System

In this existing system author is using Honeypot server to detect and prevent attacks. Honeypot is an additional server which sit between user and original server and whenever any user send request then Honeypot will intercept that request and authenticate user and his request and if user authenticated then it allows user to access original server.
If user is not authenticated and send request with fake password then Honeypot will monitor all his activity and serve him blank page.

D. Disadvantages of Existing System

- They Will Not Prevent Incidents by Themselves
- They do not Process Encrypted Packets.
- IP Packets Can Still Be Faked.
- Traffic Hijacking.
- Insecure Interface and APIs.
- Denial of Service.
- Malicious Insiders.

E. Proposed System

In proposed system author designing Honeypot server which accept user request to upload, download and share file. While sharing file users will give sharing permission and password to genuine users and then share users can give password to download file. If any malicious user tries to download file with fake password, then Honeypot server will serve him fake file to gather more information from the user and the honeypot server will block the Ip address permanently.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

F. Advantages of Proposed System

- They Can Be Tuned to Specific Content in Network Packets.
- They Can Qualify and Quantify Attacks.
- They Make It Easier to Keep Up with Regulation.
- Proposes a new technique of protecting data and resources in a cloud through Honeypot.
- The application makes it possible to store as well as share a document.

III. THE ARCHITECTURE OF THE PROJECT

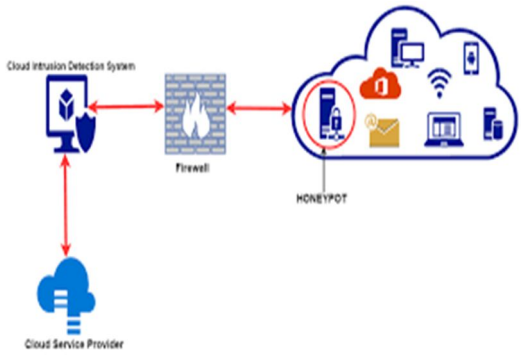


Fig 1: System Architecture

The term “the cloud” is used as a metaphor for the Internet, based on the fact that a cloud like shape was used to indicate network telephone schematics, and later the Internet as an abstraction of underlying infrastructure it represents. Honeypots are viewed as a successful technique to track programmer conduct and uplift the viability of security instruments. Honeypots are specifically designed to not only purposely engage and deceive hackers but also identify malicious activities performed over the Internet and can be counted as an effective method to track hacker behavior.

1) Implementation

A.NEW USER REGISTER
In this module user will register

B. UPLOAD FILE
In this module user will upload file.

C. LOGIN
In this module user will login.

D. DOWNLOAD FILE
In this module user will download file.

2) Test cases and Scenarios

TEST CASE ID	TYPE OF TESTCASE	DESCRIPTION	INPUT	REMARKS
1	Unit testing	User Signup/Login	Details	Testcase success
2	Unit testing	Upload file	--	Testcase success
3	Unit testing	Data visualization	--	Testcase success
4	Unit testing	Upload test tweets	Text file	Testcase success
5	Unit testing	response	--	Testcase success

IV. CONCLUSION & FUTURE SCOPE

Any Organization or firm with either outside resources/areas or cloud administrations ought to deploy cloud-based Honeypots. The IT staff might be required to arrange the Honeypots, yet the genuine outline ought to be driven by the security groups will's identity observing for vindictive movement. Any association managing delicate information in the cloud must prefer Honeypots, and they will likewise require talented system heads to screen the logs and respond to the information. There are some incredible open-source apparatuses that have been created to help with the observing and log gathering of Honeypots. "The perfect Honeypot for Amazon EC2 will contrast from Microsoft's Azure or IBM's cloud".

Cloud-based Honeypots give the capacity to explore and examine assaults that hit ordinary customers. Having them permits a specialist to interpret the IP locations and malware being utilized into security content that can ensure a normal cloud environment. Once those IP addresses have been distinguished, they will then lead a ping scope and defenselessness output to discover a shortcoming in the system outline or vulnerabilities in programming that can be misused. It's conspicuous yet genuine; awful folks pursue the weakest focuses the most often. There are upsides of utilizing a cloud construct Honeypot in light of a cloud framework is like customary Honeypots in that it ought to have the capacity to decide whether a cloud framework has been traded off or endeavors were made to do so.

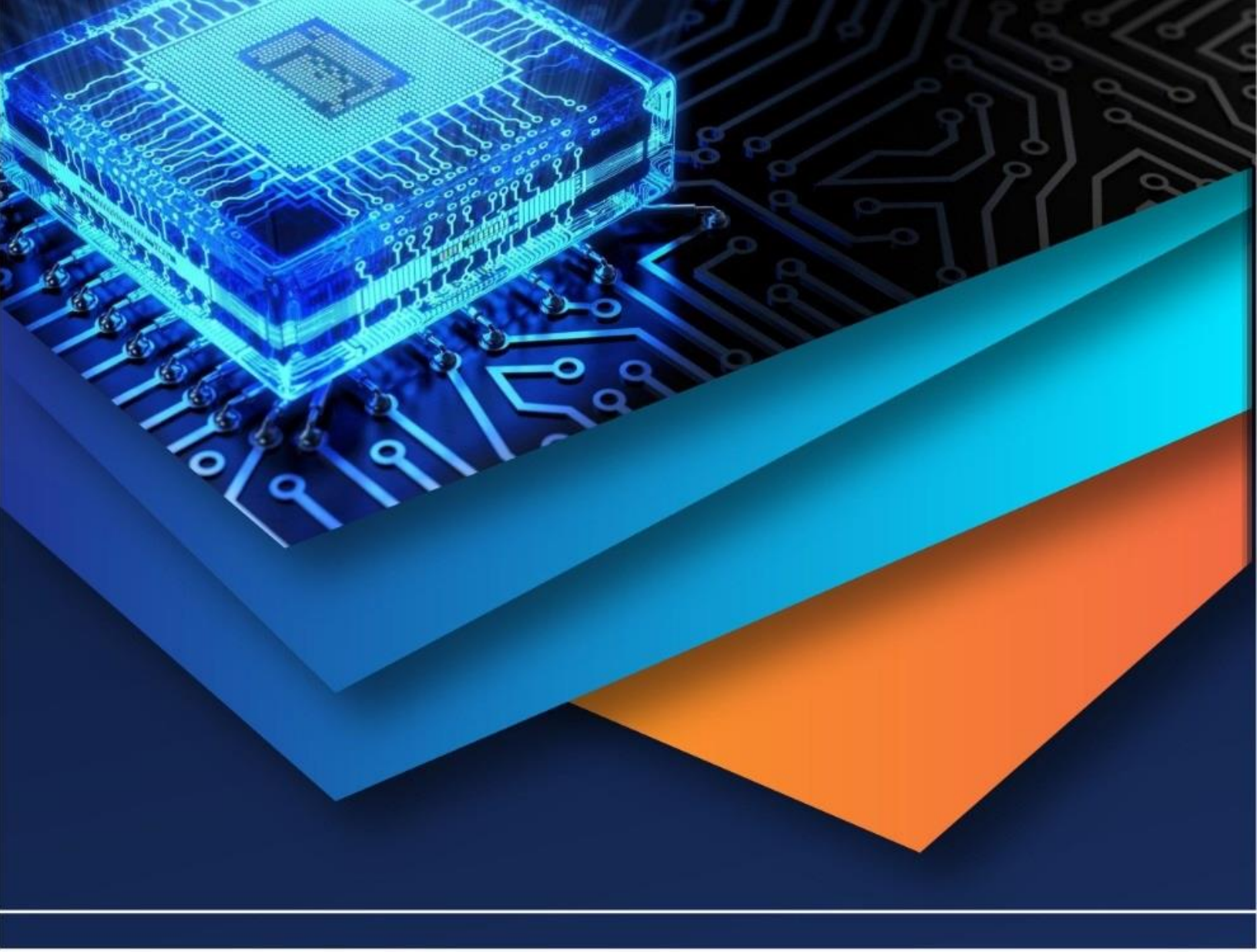
Cloud is one of the few technologies that can bring about a major change, hence it is very necessary to make security of cloud stronger. We present a way to tackle malicious users using honeypot. Organizations can prefer using honeypot for detection of rogue elements. One can easily understand the behavior of an attacker by implementing it. Since risks are increasing day-by-day. technology extra efforts are required to be put-in. Honeypot ensures extra security and detection feature which can be further increased in standard as the technology advances.

REFERENCES

[1] RuWei Huang, Si Yu, Wei Zhuang and XiaoLinGui, “Design of Privacy-Preserving Cloud Storage Framework 2010 Ninth International Conference on Grid and Cloud Computing.
[2] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., “Scientific Cloud Computing: Early Definition and Experience,” 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825- 830, Dalian, China, Sep. 2008
[3] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou, “Ensuring Data Storage Security in Cloud Computing”, In Quality of Service, 2009. 17th International Workshop on, page 19, 2009.
[4] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou “Ensuring Data Storage Security in Cloud Computing.” IEEE 2009.
[5] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. Atanu Rakshit, “Cloud security issues” In Services Computing, 2009. IEEE International Conference on, page 517520, 2009. Kashish Goyal, SupriyaKinger” Modified Caesar Cipher for Better Security Enhancement” International Journal of Computer Applications (0975– 8887) Volume 73– No.3, July 2013.
[6] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,” Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures” IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.
[7] Mr. Gurjeevan Singh, Mr. Ashwani Singla and Mr. K S Sandhi “Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System” International Journal of Multidisciplinary ResearchVol.1 Issue 4, August 2011.
[8] D. S. Abdul. Elmina am, H. M. Abdul Kader and M. M. Hadhoud,“ Performance Evaluation of Symmetric Encryption Algorithms”, Communications of the IBIMA Volume 8, 2009.
[9] Gurpreet Singh, Supriya Kinger” Integrating AES, DES, and 3 -DES Encryption Algorithms for Enhanced Data Security “International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

WEBSITES:

https://www.W3schools.Com/python/
https://www.Tutorialspoint.Com/python/index.Htm
https://www.Javatpoint.Com/python-tutorial
https://www.Learnpython.Org/
https://www.Pythontutorial.Net/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY