SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
*Deemed to be University u/s 3 of UGC Act, 1956*

# Honeypot Implementation in Cloud Environ with Open Source Medium

Guide Name: Dr. G. Senthil Kumar (100195)

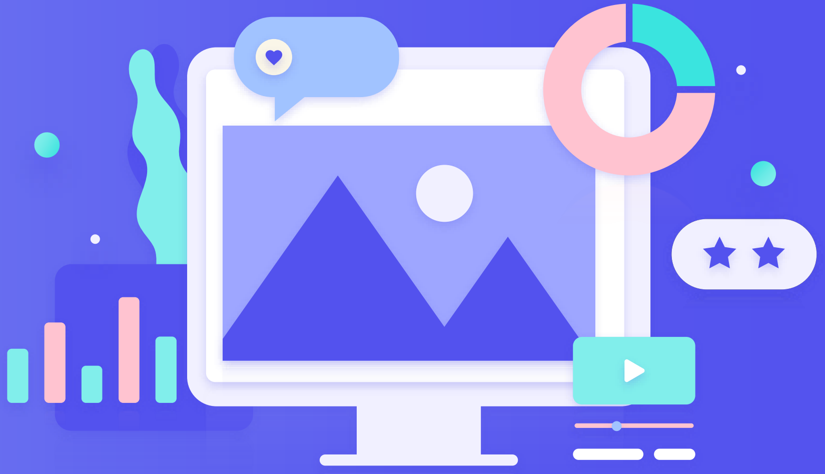
K. Dushyant Reddy Regno. RA1911033010029
Siddharth Chakraborty Regno. RA1911033010048

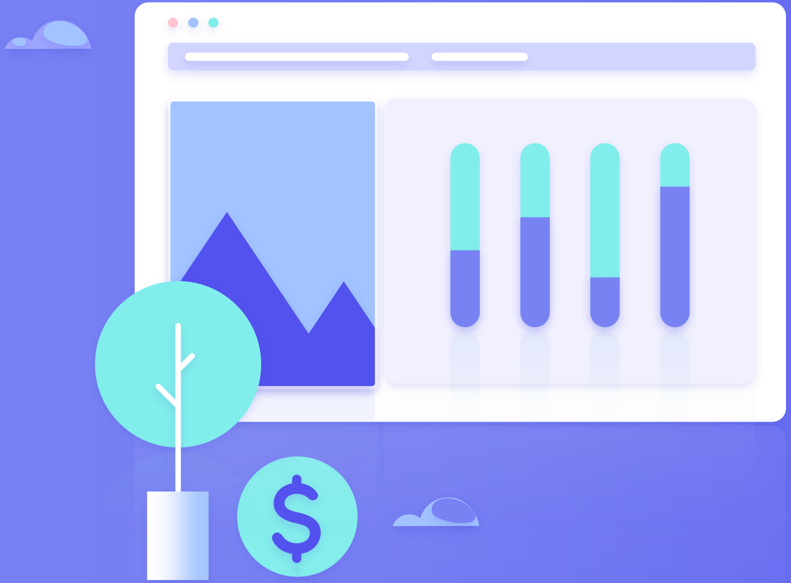
# Table of Contents

| S NO. | TITLE |
|---|---|
| 01 | Introduction |
| 02 | Motivation/Objective |
| 03 | Project Idea/Problem Statement |
| 04 | Purpose |
| 05 | Scope |
| 06 | Requirement Gathering |
| 07 | Literature Survey |
| 08 | Limitations |
| 09 | Proposed System Architecture Diagram |

# Introduction

Honeypots can provide a valuable cybersecurity information. But is it worth the risk? A network-attached machine called a honeypot is set up as a ruse and is intended to mimic a server or other high-value asset. Its goal is to stop hacking efforts that may have otherwise resulted in illegal access to information systems. A honeypot operation often comprises of a computer, apps, and data that mimic the behaviour of a genuine system, such a banking system or IoT devices, but are entirely isolated and closely watched.





# Motivation

The main motivation to start this project was to understand the pattern of cyber attacks and ransomware attacks on a cloud system so that the vulnerability could be reduced. The majority of organisations in the government, military, and research use research honeypots. They are gathering an enormous amount of data. They want to find new dangers and learn more about Blackhat practises and motivations. They don't directly contribute to an organization's security; rather, the goal is to learn how to safeguard systems more effectively.

# Project Idea

Our target in doing this research is to better understand how security systems function, how to defend a business, and the dangers of system security defects. We'll discover how a system functions and how it may be improved. Once we obtain the results, we will use forensic science instruments to assess the output. We will run into some issues when attempting all of them, and we will work to fix them. We will also have experience developing and running these kinds of systems in the future. If a network has comparable issues, we will be able to manage the situation and make up for the loss.

About Web Companies

Them

It's the closest planet to the Sun and the smallest one in the Solar System—it's only a bit larger than the Moon

Us

Venus has a beautiful name and is the second planet from the Sun. It's hot and has a poisonous atmosphere

# Purpose

The main purpose of the honeypot system is to refine the performance of the threat detection system of any cloud service by managing and preventing attacks. The software will be used by the team to ensure network safety for the cloud.

# Scope

Our perspective is to find solutions to issues with security, the use of honeypots, and the volume of data we can gather. We'll examine the rules that apply to honeypot installation constraints, as well as how far a network security administrator can go to gather data and find the hacker, with a focus on India. We'll provide explanations and generate some discussion about what should be done in accordance with the law and what shouldn't. Based on our study, we will have some opinions and recommendations. While searching for solutions to security issues, we will also assess and consider the experiment limitations.

# Requirement Gathering

## Functional

| ID | Requirement |
|---|---|
| FR1.1 | A system that combines constant anomalous network activity with deception strategies. |
| FR1.2 | An system emulator with settings that mimic different vulnerable systems |
| FR1.3 | Coverage for all devices that are known targets of malicious activities |
| FR1.4 | Full activity logging for data protection standards compliance |

# Requirement Gathering

## Non - Functional

| ID | Requirement |
|---|---|
| NFR1.1 | The process of research should be secure and should not have any valuable data. |
| NFR1.2 | The process should be scalable which means that it must have some future scope where it can be expanded. |
| NFR1.3 | The process should be reliable and continue throughout the stipulated time period. |
| NFR1.4 | The process must be portable so that the research can be implemented on any system anywhere. |

# Literature Survey

| Year | Publication Details | Approach | Limitations |
|---|---|---|---|
| 2018 | Almohannadi, Hamad, Irfan Awan, Jassim Al Hamar, Andrea Cullen, Jules Pagan Disso, and Lorna Armitage. "Cyber threat intelligence from honeypot data using elasticsearch." In *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, pp. 900-906. IEEE, 2018. | A new threat intelligence technique which is evaluated by analyzing honeypot log data to identify behavior of attackers to find attack patterns.<br>IPS systems generate alerts and prevent cyber attacks. | It requires greater intelligence in order to fully understand an adversary's motive by analyzing various types of Indicator of Compromise (IoC).<br>It is important for the IT employees to have enough knowledge to identify true positive attacks and act according to the incident response process |

# Literature Survey

| Year | Publication Details | Approach | Limitations |
|---|---|---|---|
| 2022 | Alyas, Tahir, Khalid Alissa, Mohammed Alqahtani, Tauqeer Faiz, Suleiman Ali Alsaif, Nadia Tabassum, and Hafiz Hasan Naqvi. "Multi-Cloud Integration Security Framework Using Honeypots." *Mobile Information Systems* 2022 (2022). | The transformation of this digital ecosystem is heavily dependent on cloud computing, as it is becoming the global platform for individuals, corporates, and even governments.<br>This mechanism is designed using the honeypot technology that has been around for some time but has not been used in cloud computing and other technologies. | One essential and integral segment of this progress is the security concerns related to data at rest, in transit, and the attacks and compromises on digital assets. |

# Literature Survey

| Year | Publication Details | Approach | Limitations |
|---|---|---|---|
| 2018 | Lihet, Marius, and Vasile Dadarlat. "Honeypot in the cloud five years of data analysis." In *2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1-6. IEEE, 2018. | All hacking attacks discovered or not can have a catastrophic result in a company or state entity.<br>The system is left intentionally vulnerable to the attackers in order to study and analyze the techniques and tools used by the attacker. | Complexity and the adoption of more and more computer based software or hardware into the daily life of big companies has paid its tool to hackers.<br>Corporate environment lots of big names were affected and lost millions of dollars directly or indirectly after they were hacked |

# Literature Survey

| Year | Publication Details | Approach | Limitations |
|---|---|---|---|
| 2018 | Krishnaveni, S., S. Prabakaran, and S. Sivamohan. "A survey on honeypot and honeynet systems for intrusion detection in cloud environment." *Journal of Computational and Theoretical Nanoscience* 15, no. 9-10 (2018): 2949-2953. | Honeynet is network architecture that is meant to deceive an attacker and capture their techniques for further analysis of the attacking session, they have been evolving through the last two decades, but without coping with the continuously advanced adversaries' techniques. | A new security technique may cause a network and performance overhead that might affect the underlined service and thus increase the latency dramatically.<br>There have been issues in the current honeypot cloud system which leaves space for some vulnerabilities. |

# Literature Survey

| Year | Publication Details | Approach | Limitations |
|---|---|---|---|
| 2019 | Saxena, Ms Apurva, Gaurav Ubnare, and Anubha Dubey. "Virtual Public Cloud Model in Honeypot for Data Security: A New Technique." In *Proceedings of the 2019 5th International Conference on Computing and Artificial Intelligence*, pp. 66-71. 2019. | Honeypot works in a Cloud environment where anything like technology, tools, and results can be offered as a service.<br>Implementation of high-interaction honeypot with Kerberos authentication system, VPC, VPN and EFS as a service in cloud environment to provide overall security to the data/network. | The duplicated hacker behavior may be redundant and not cover all the different test cases which would be present in the scope of the study. |

# Literature Survey

| Year | Publication Details | Approach | Limitations |
|---|---|---|---|
| 2021 | Maesschalck, Sam, Vasileios Giotsas, Benjamin Green, and Nicholas Race. "Don’t get stung, cover your ICS in honey: How do honeypots fit within industrial control system security." *Computers & Security* (2021): 102598. | Honeypots can be integrated within an organisation's defensive strategy.<br>The increased knowledge attackers have on how real-world ICS devices are configured and operate vs the configurability of simulated honeypot systems | Many low-interaction honeypots are limited in their use.<br>Environments with increased interaction provide more extensive capabilities and value, due to their inherent obfuscation delivered through the use of real-world systems. |

# Literature Survey

| Year | Publication Details | Approach | Limitations |
|---|---|---|---|
| 2012 | Borisaniya, Bhavesh, Avi Patel, Dhiren R. Patel, and Hiren Patel. "Incorporating honeypot for intrusion detection in cloud infrastructure." In *IFIP International Conference on Trust Management*, pp. 84-96. Springer, Berlin, Heidelberg, 2012. | Cloud services delivered as utility computing over the Internet makes it an attractive target for cyber intruders.<br>Introducing Honeypot in Cloud IDS design can greatly help in detecting potential attacks with reduced number of false positives. | Traditional Anomaly Detection based IDS may generate more false positives.<br>Most of the Network based Intrusion Detection System (NIDS) being rule based and therefore only capable of identifying known attacks |

# Literature Survey

| Year | Publication Details | Approach | Limitations |
|---|---|---|---|
| 2021 | Susukailo, V., S. Vasylyshyn, I. Opirskyy, V. Buriachok, and O. Riabchun. "Cybercrimes investigation via honeypots in cloud environments." In *CEUR Workshop Proceedingsthis link is disabled*, vol. 2923, pp. 91-96. 2021. | Analyses the problem of cybercrimes investigation in cloud environments.<br>Examines appropriate technologies used by cybersecurity professionals during the cybercrimes investigation. Identifies advantages of honeypots usage in cloud infrastructure. | Cloud environments can give organizations the freedom to experiment and scale the resources, it also increases the attack surface.<br>Information is very scarce, and it sorely lacks to prevent further the emergence of threats to the security of protected information resources |

# Literature Survey

| Year | Publication Details | Approach | Limitations |
|---|---|---|---|
| 2017 | Mahajan, Varan, and Sateesh K. Peddoju. "Integration of network intrusion detection systems and honeypot networks for cloud security." In *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 829-834. IEEE, 2017. | The methods of detection of intrusion and deployment of NIDS in cloud environments are dependent on the type of services being rendered by the cloud.<br>The cloud administrator is able to determine the malicious intentions of the attackers and various methods of attack. | Method to generate and update signatures from information derived from the proposed integrated model.<br>Overhead due to multiple instances of NIDS running in the Cloud environment and methods to achieve balance between performance and security. |

# Literature Survey

| Year | Publication Details | Approach | Limitations |
|---|---|---|---|
| 2022 | Alwaheidi, Mohammed KS, and Shareeful Islam. "Data-Driven Threat Analysis for Ensuring Security in Cloud Enabled Systems." *Sensors* 22, no. 15 (2022): 5726. | Cloud computing offers many benefits including business flexibility, scalability and cost savings but despite these benefits, there exist threats that require adequate attention for secure service delivery. | Threats and vulnerabilities relating to the cloud services can pose potential risks.<br>There are a number of threat analysis techniques but a lack of focus on the comprehensive understanding of data for threat analysis is apparent. |

# Literature Survey

| Year | Publication Details | Approach | Limitations |
|---|---|---|---|
| 2018 | Jafirkhan, Mu Ateek Mu, and Shubhangi Mahadik. "Data Security using Honeypot System." (2018). | An asset used to trap assaults, records interruption data about occasions of the hacking procedure, and dodges assault outbound the traded off PC framework.<br>Records exercises of the hacking interruption data about instruments and exercises of the hacking procedure. | Honeypots don't create erroneous alarms or log records like other interruption identification frameworks in light of the fact that no gainful parts are running on the framework. |

# Literature Survey

| Year | Publication Details | Approach | Limitations |
|---|---|---|---|
| 2019 | Akhtar, Jahanara, Md Tahzib-Ul-Islam, Md Habibullah Belali, and Saiful Islam. "Big Data Security with Access Control Model and Honeypot in Cloud Computing." *International Journal of Computer Applications* 173 (2019): 88. | Acceptance of cloud facility, numerous of the enterprises are expanding to store and process Large Data in cloud.<br>Cloud can stock a big size of data, multipart divisions, and generation of client output. | Enterprise as well as users are suffering with proper security aspects to store, retrieve and process big data in a cloud environment.<br>Technology fluctuations affect the classification changes of such data completed over a period. Therefore, it's meaning fluctuations time to time and organization to organization |

# Literature Survey

| Year | Publication Details | Approach | Limitations |
|---|---|---|---|
| 2012 | Kinariwala, Roshni M., and G. B. Jethava. "Research on Various Next Generation Honeypot Systems." *International journal of engineering research and technology* 1 (2012). | Production honeypots are primarily used and they are easy to use and they capture only a small amount of information.<br>Honeypots are the security systems which can be used to provide network security and business profit. | High-interaction honeypots are more complex and difficult for real time systems. They allow attackers to interact with real time application or systems and also capture the information for analysis of their behavior |

# Literature Survey

| Year | Publication Details | Approach | Limitations |
|---|---|---|---|
| 2018 | Baykara, Muhammet, and Resul Das. "A novel honeypot based security approach for real-time intrusion detection and prevention systems." *Journal of Information Security and Applications* 41 (2018): 103-116. | In order to ensure the security of information systems, various systems use techniques and technologies, including encryption, authorization, firewall, honeypot based systems.<br>The developed honeypot server application is combined with IDSs to analyze data in real-time and to operate effectively. | There can be some issues in the implementation of the honeypot system which means that the vulnerability and threat protection system will not be fully functional and has chances of causing malfunctions in the system. |

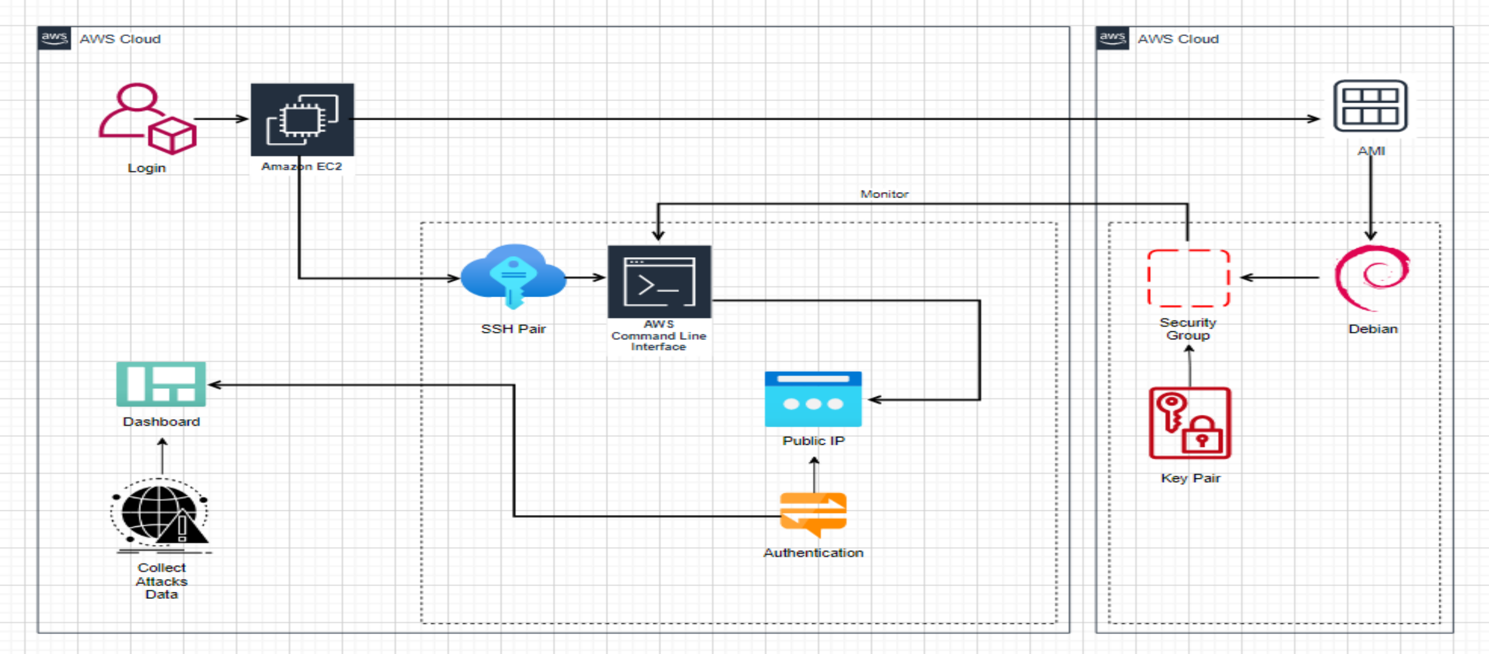
# Literature Survey

| Year | Publication Details | Approach | Limitations |
|---|---|---|---|
| 2018 | Sekar, K. R., V. Gayathri, Gollapudi Anisha, K. S. Ravichandran, and R. Manikandan. "Dynamic honeypot configuration for intrusion detection." In *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, pp. 1397-1401. IEEE, 2018. | Identify the unauthorized users and intruders in the network. The enterprise level security can be possible via high scalability.<br>Methodologies were deployed to catch the Intruders who utilizing the unsecured network through the unused IP address | The network activity and traffic can also be tracked through honeypot<br>Always with a caution and threat the intruders roaming in the un secured network. |

# Research Limitation

- The research is limited in some directions because the reach of the honeypot system is quite limited and this means that it cannot map out the attack patterns for all the different areas.
- There are implementation issues as well because the access to the required technologies is quite limited.
- The issue is also present with the ackers because they have developed their knowledge of the current system it might be difficult to have them attack the honeypot cloud server.

# Proposed System Architecture Diagram

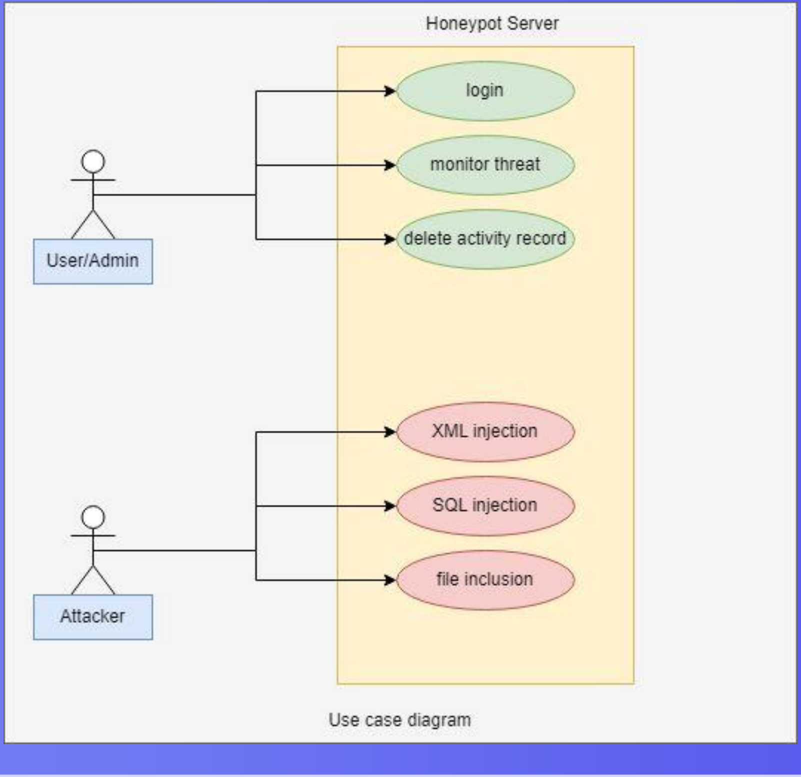


Proposed System Architecture Diagram

# Cont.

To begin, sign in to your AWS account and choose the region where you wish to host the honeypot. To start a new instance, go to the EC2 service. Choose Debian 10 Buster from the AWS Marketplace to make sure it can store many honeypots that are running in docker containers as well as the elk stack that will be used to monitor assaults. The next step is to launch instance by either choosing an existing pair or building a new one. Transferring the key pair from the host to the VM will now allow you to login to the instance from the virtual machine. Launch the CLI after initialization to verify the user's credentials and execute the code to retrieve the data for the dashboard that shows the attacks.

# Detail Design Diagram - Use Case Diagram



# Cont.

At its most basic level, a use case diagram shows how a user engages with the system and details the requirements of a use case. Obtaining data from an input packet.

Involvement in Selective Circumstances

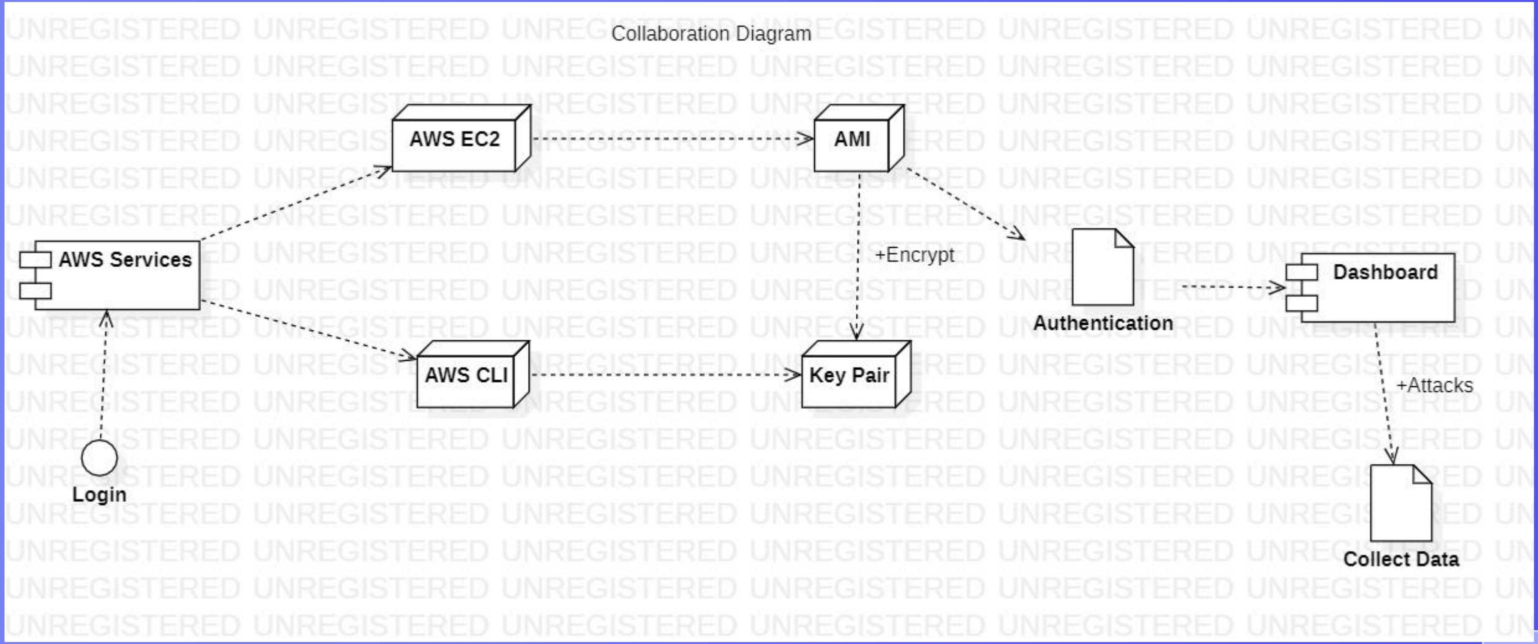
**User:**

- Enrol
- Threat auditing
- Eliminate the activity log

**Attacker:**

- SQL injection
- Allocation of File
- XML injection

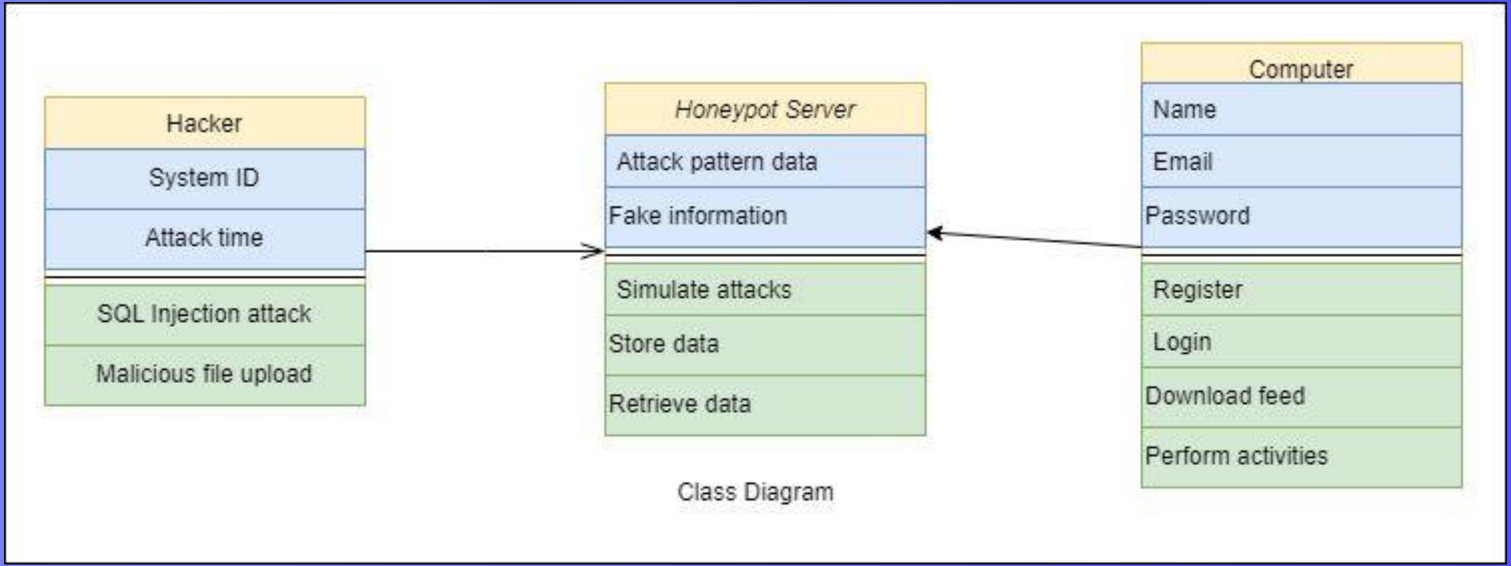
# Detail Design Diagram - Collaboration Diagram



# Cont.

The breakdown of components into a lower-level structure or when you are separating your System into components and want to illustrate how they interact through Interfaces. It explains a system's static structure as well as its dynamic behaviour by illustrating interactions between dashboard or threat data in terms of sequenced messages.

# Detail Design Diagram - Class Diagram



Hacker

System ID

Attack time

SQL Injection attack

Malicious file upload

*Honeypot Server*

Attack pattern data

Fake information

Simulate attacks

Store data

Retrieve data

Computer

Name

Email

Password

Register

Login

Download feed

Perform activities

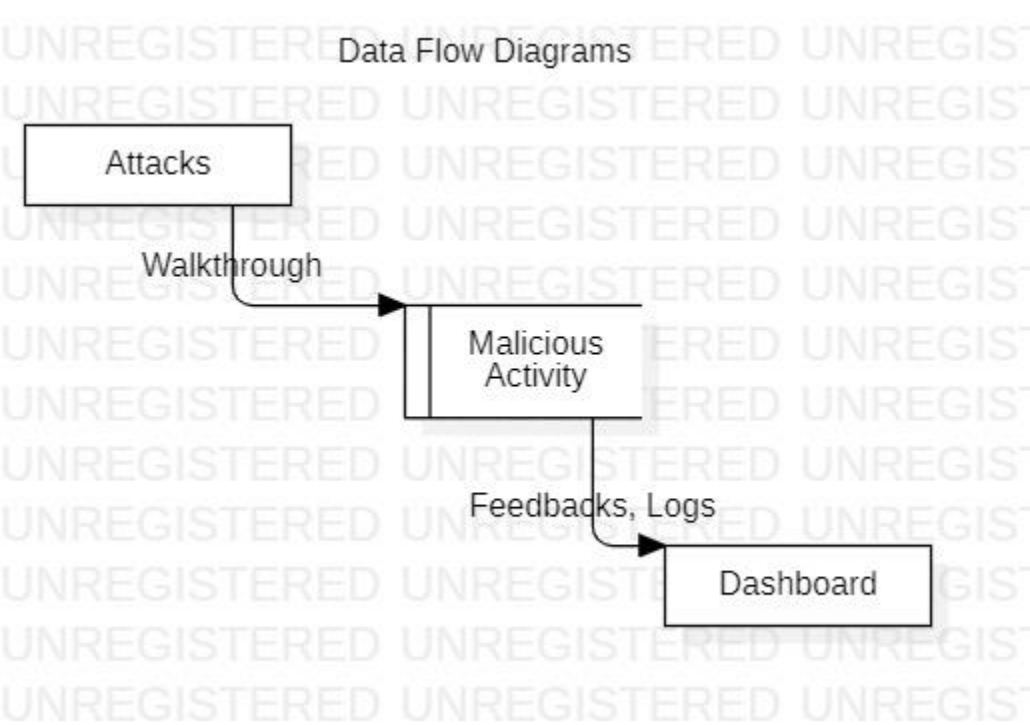
Class Diagram

# Cont.

For honeypots, a class diagram outlines the kind of data or characteristics that are retained in each ”class,” the functions or capabilities that each class provides, and the relationships between the classes. Shows a hacker, a honeypot server, and a personal computer. The qualities of the hacker include attack time and a variable ID that malfunctions to produce false information about the attack while simulating the retrieval and saving of data. Obtaining the feed data and doing out tasks.

Additionally, it enables the simulation of virtual network topologies through the employment of a routing mechanism that imitates various network properties, including delay and latency.

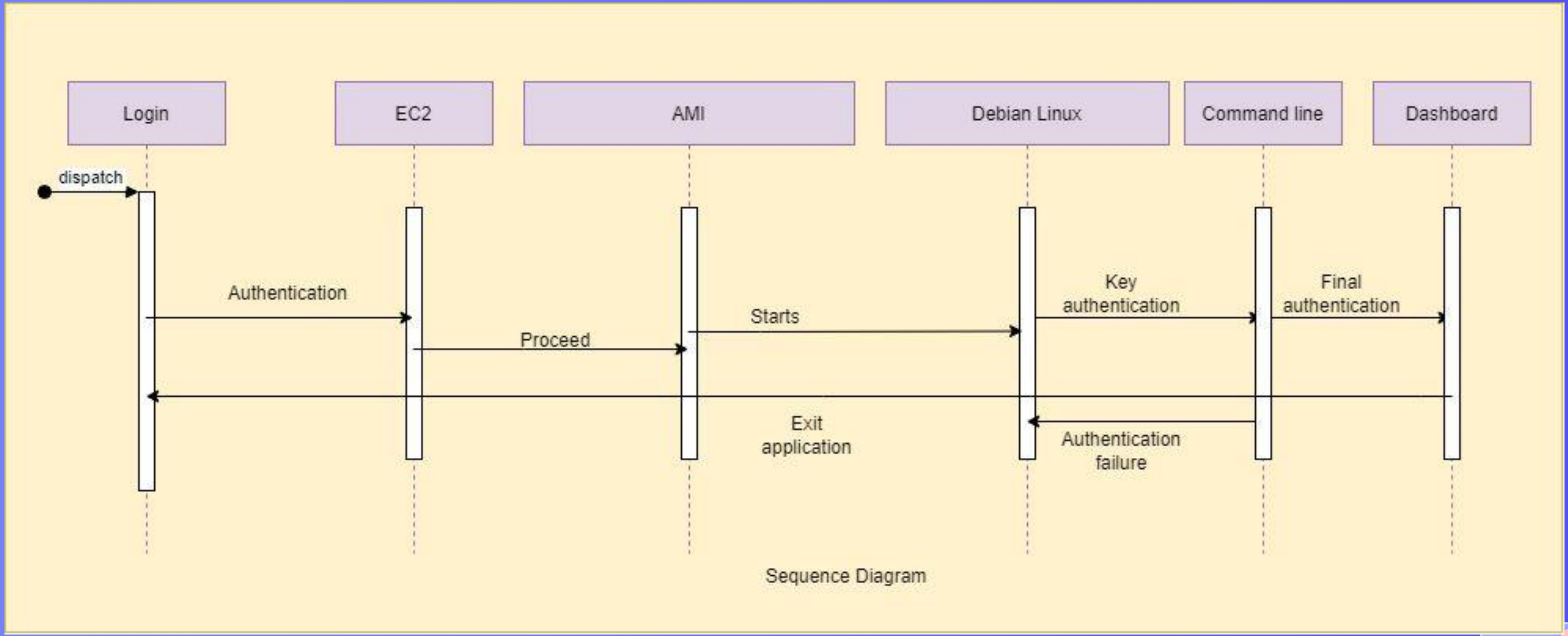
# Detail Design Diagram - Data Flow Diagram



# Cont.

Data flow diagrams in honeypot describes the walkthrough within a software or system, the complete data movement process is mapped as it moves from one component to the next, taking into account how the attacked changes form during the malicious activity. They are utilised to assess the threats that businesses face and how to better guard against such threats. Then, Network Administrators are required to submit the network's range and a plug-in that is specific to each honeypot.

# Detail Design Diagram - Sequence Diagram



# Cont.

Demonstrates how EC2 and the CLI communicate with one another. When an attacker opens a secure connection to the SSH proxy, the interaction begins. The attacker can attempt to log in after the connection has been made using a username and password. After successful authentication, the attacker can issue orders to the proxy. The decision-making module, which implements the learning algorithm as outlined in Algorithm, will be queried for a response by the proxy after it has examined the request.

# Module Description

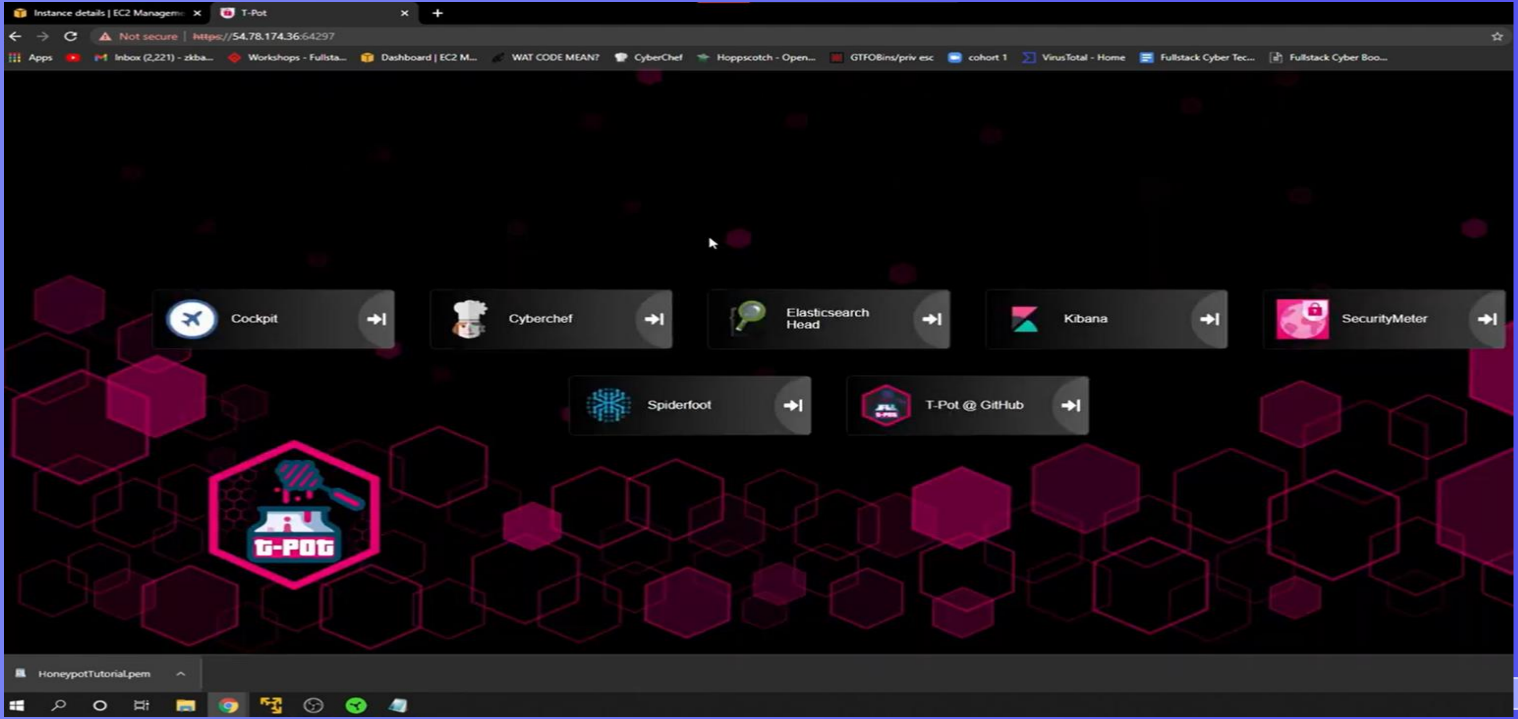
The report will be revealed in the log that the honeypot creates:

a. IP address
b. Inside this teapot, there are accessible honey pots.
c. Assaults by time or place
d. Attacks using the attacking ips command input
e. Attacks through SRCIP and ASN

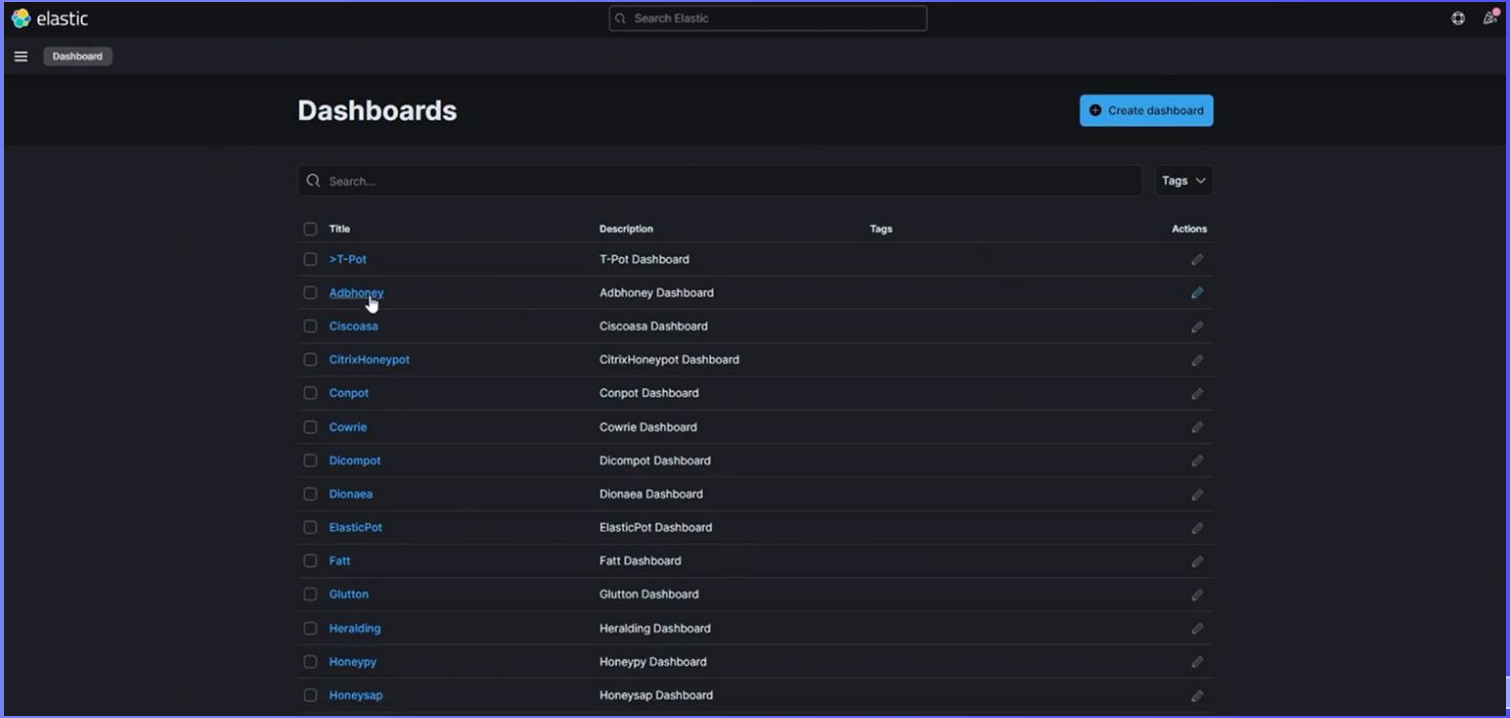
# Results & Discussions

The result for the honeypot system was properly identified and based on the implementation of the honepot we were able to properly find out the expected results and based on that we were able to match the research expectations which allowed us to fulfill the research objectives as well and it had become quite easy to answer all the relevant research questions based on which the discussion for the research purpose was also fulfilled.

# Screenshots



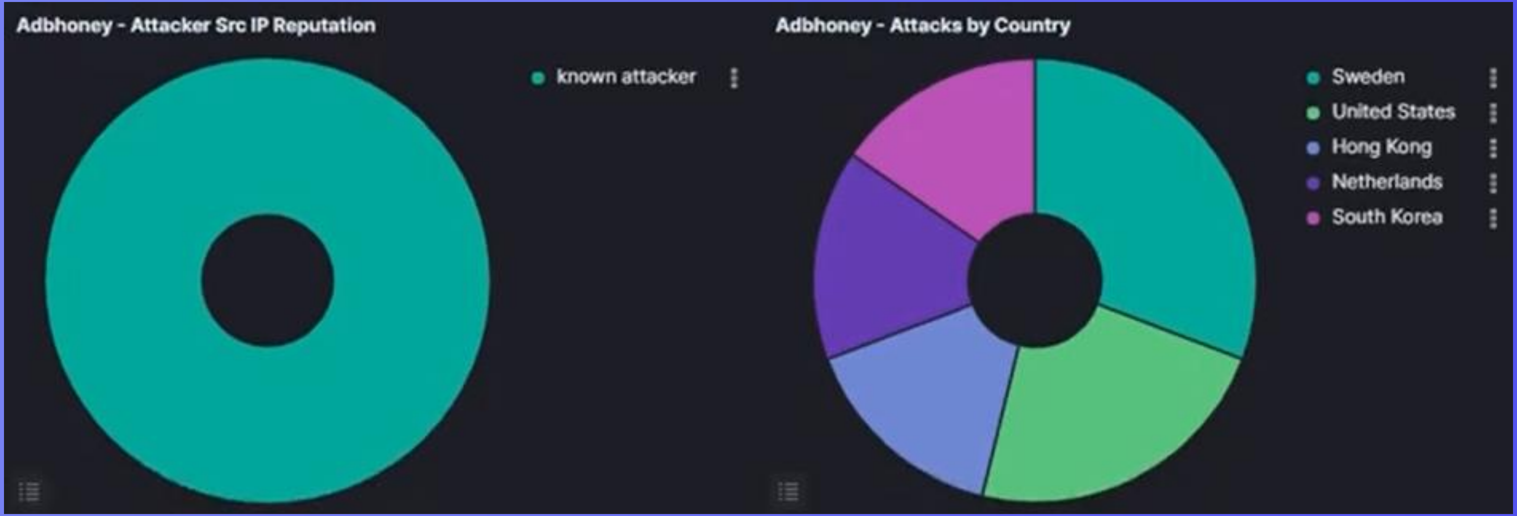
# Kibana Dashboard



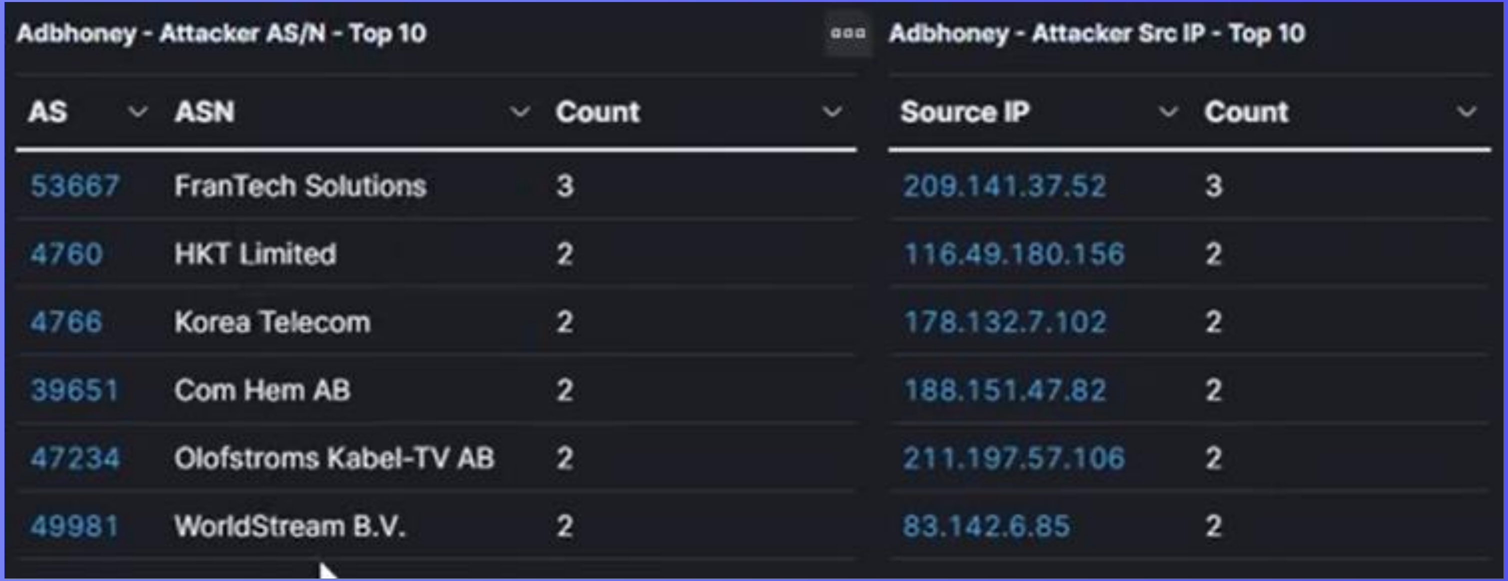
## Dashboards

| ☐ Title | Description | Tags | Actions |
|---|---|---|---|
| ☐ >T-Pot | T-Pot Dashboard | | ✎ |
| ☐ Adbhoney | Adbhoney Dashboard | | ✎ |
| ☐ Ciscoasa | Ciscoasa Dashboard | | ✎ |
| ☐ CitrixHoneypot | CitrixHoneypot Dashboard | | ✎ |
| ☐ Conpot | Conpot Dashboard | | ✎ |
| ☐ Cowrie | Cowrie Dashboard | | ✎ |
| ☐ Dicompot | Dicompot Dashboard | | ✎ |
| ☐ Dionaea | Dionaea Dashboard | | ✎ |
| ☐ ElasticPot | ElasticPot Dashboard | | ✎ |
| ☐ Fatt | Fatt Dashboard | | ✎ |
| ☐ Glutton | Glutton Dashboard | | ✎ |
| ☐ Heralding | Heralding Dashboard | | ✎ |
| ☐ Honeypy | Honeypy Dashboard | | ✎ |
| ☐ Honeysap | Honeysap Dashboard | | ✎ |

# Graphs


Adbhoney - Attacker Src IP Reputation
● known attacker
Adbhoney - Attacks by Country
● Sweden
● United States
● Hong Kong
● Netherlands
● South Korea

# ASN and SRCIP Address



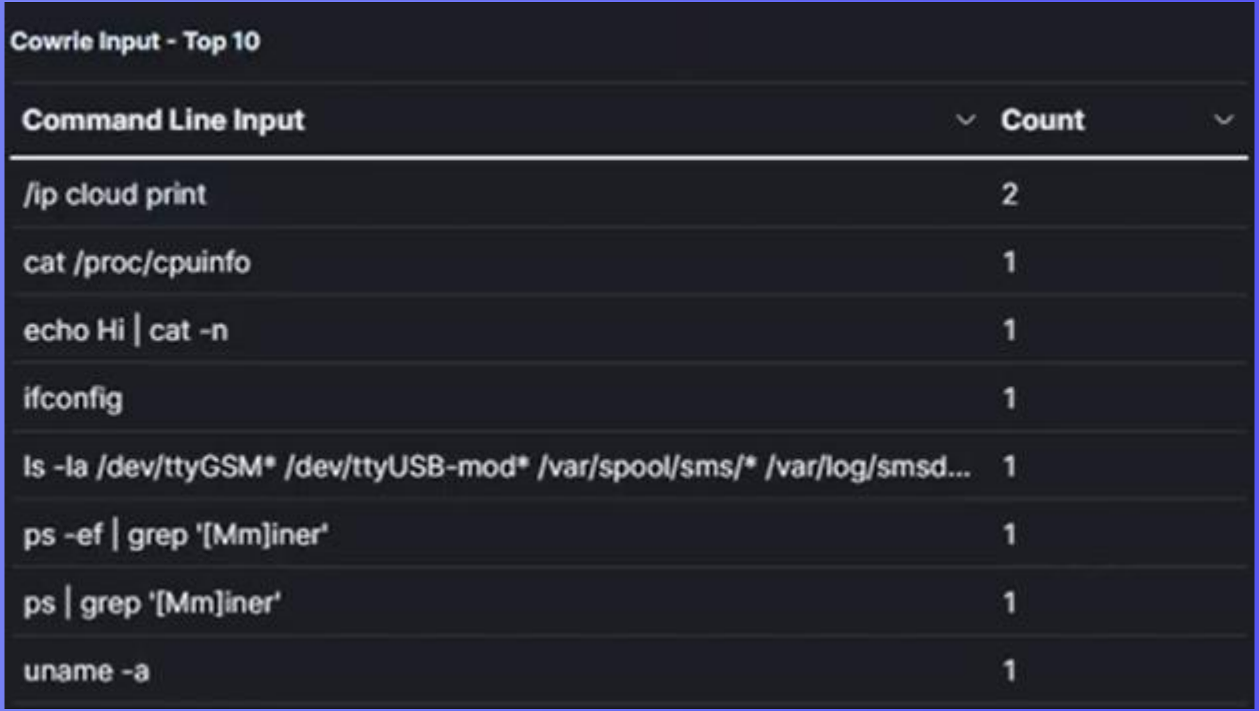
Adbhoney - Attacker AS/N - Top 10

| AS | ASN | Count |
|---|---|---|
| 53667 | FranTech Solutions | 3 |
| 4760 | HKT Limited | 2 |
| 4766 | Korea Telecom | 2 |
| 39651 | Com Hem AB | 2 |
| 47234 | Olofstroms Kabel-TV AB | 2 |
| 49981 | WorldStream B.V. | 2 |

Adbhoney - Attacker Src IP - Top 10

| Source IP | Count |
|---|---|
| 209.141.37.52 | 3 |
| 116.49.180.156 | 2 |
| 178.132.7.102 | 2 |
| 188.151.47.82 | 2 |
| 211.197.57.106 | 2 |
| 83.142.6.85 | 2 |

# CLI Input Attack Counts



Cowrie Input - Top 10

| Command Line Input | Count |
|---|---|
| /ip cloud print | 2 |
| cat /proc/cpuinfo | 1 |
| echo Hi \| cat -n | 1 |
| ifconfig | 1 |
| ls -la /dev/ttyGSM* /dev/ttyUSB-mod* /var/spool/sms/* /var/log/smsd... | 1 |
| ps -ef \| grep '[Mm]iner' | 1 |
| ps \| grep '[Mm]iner' | 1 |
| uname -a | 1 |

# References

Almohannadi, Hamad, Irfan Awan, Jassim Al Hamar, Andrea Cullen, Jules Pagan Disso, and Lorna Armitage. "Cyber threat intelligence from honeypot data using elasticsearch." In *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, pp. 900-906. IEEE, 2018.

Lihet, Marius, and Vasile Dadarlat. "Honeypot in the cloud five years of data analysis." In *2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1-6. IEEE, 2018.

Alyas, Tahir, Khalid Alissa, Mohammed Alqahtani, Tauqeer Faiz, Suleiman Ali Alsaif, Nadia Tabassum, and Hafiz Hasan Naqvi. "Multi-Cloud Integration Security Framework Using Honeypots." *Mobile Information Systems* 2022 (2022).

Krishnaveni, S., S. Prabakaran, and S. Sivamohan. "A survey on honeypot and honeynet systems for intrusion detection in cloud environment." *Journal of Computational and Theoretical Nanoscience* 15, no. 9-10 (2018): 2949-2953.

Saxena, Ms Apurva, Gaurav Ubnare, and Anubha Dubey. "Virtual Public Cloud Model in Honeypot for Data Security: A New Technique." In *Proceedings of the 2019 5th International Conference on Computing and Artificial Intelligence*, pp. 66-71. 2019.

# References

Maesschalck, Sam, Vasileios Giotsas, Benjamin Green, and Nicholas Race. "Don’t get stung, cover your ICS in honey: How do honeypots fit within industrial control system security." *Computers & Security* (2021): 102598.

Mahajan, Varan, and Sateesh K. Peddoju. "Integration of network intrusion detection systems and honeypot networks for cloud security." In *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 829-834. IEEE, 2017.

Susukailo, V., S. Vasylyshyn, I. Opirskyy, V. Buriachok, and O. Riabchun. "Cybercrimes investigation via honeypots in cloud environments." In *CEUR Workshop Proceedingsthis link is disabled*, vol. 2923, pp. 91-96. 2021.

Alwaheidi, Mohammed KS, and Shareeful Islam. "Data-Driven Threat Analysis for Ensuring Security in Cloud Enabled Systems." *Sensors* 22, no. 15 (2022): 5726.

Borisaniya, Bhavesh, Avi Patel, Dhiren R. Patel, and Hiren Patel. "Incorporating honeypot for intrusion detection in cloud infrastructure." In *IFIP International Conference on Trust Management*, pp. 84-96. Springer, Berlin, Heidelberg, 2012.

# References

Jafirkhan, Mu Ateek Mu, and Shubhangi Mahadik. "Data Security using Honeypot System." (2018).

Akhtar, Jahanara, Md Tahzib-Ul-Islam, Md Habibullah Belali, and Saiful Islam. "Big Data Security with Access Control Model and Honeypot in Cloud Computing." *International Journal of Computer Applications* 173 (2019): 88.

Baykara, Muhammet, and Resul Das. "A novel honeypot based security approach for real-time intrusion detection and prevention systems." *Journal of Information Security and Applications* 41 (2018): 103-116.

Kinariwala, Roshni M., and G. B. Jethava. "Research on Various Next Generation Honeypot Systems." *International journal of engineering research and technology* 1 (2012)

Sekar, K. R., V. Gayathri, Gollapudi Anisha, K. S. Ravichandran, and R. Manikandan. "Dynamic honeypot configuration for intrusion detection." In *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, pp. 1397-1401. IEEE, 2018.

# Thank You