IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

Network Intrusion Detection System Using Honeypot in cloud

Lakshmeswari Chenngiri [1], Navya Janyavula[2], Siva naredla[3], Duggempudi venkateswarlu[4], G Vijaya Simha Reddy[5]

[1] Assistant Professor, Department of Computer Science Engineering, Chalapathi Institute of Engineering and Technology, Chalapathi Rd, Nagar, Lam, Guntur, Andhra Pradesh- 522034

[2,3,4,5] Students, Department of Computer Science Engineering, Chalapathi Institute of Engineering and Technology, Chalapathi Rd, Nagar, Lam, Guntur, Andhra Pradesh- 522034

Email id: lakshmi.chennagiri@gmail.com[1], navyajanyavula3@gmail.com[2], siva.naredla14@gmail.com[3], duggempudivenkateswarlu274@gmail.com[4], g.vsreddy014@gmail.com[5]

Abstract:

The rapid growth in internet usage has led to a surge in cybercrime, data breaches, and site-hosting vulnerabilities, posing significant challenges to online security. Cloud computing has become a key solution, offering reliable, scalable, and cost-effective services, but it also introduces new security risks due to its open and interconnected nature. As cyber threats evolve, the need for advanced intrusion detection systems has become more pressing. Honeypots, decoy systems designed to lure attackers, have proven to be an effective tool for identifying malicious activity and diverting harmful traffic away from critical infrastructure. However, the effectiveness of honeypots in cloud environments can be enhanced by leveraging machine learning models for more accurate and efficient intrusion detection. This study investigates the integration of machine learning models, specifically Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN), to improve the detection of intrusions in cloud-based honeypots. By analyzing large datasets of network traffic, the models were trained to distinguish between normal and malicious activity. The results demonstrate that the RNN model achieved an accuracy of 93.29%, while the CNN model reached 91.57%, highlighting their potential for high-accuracy intrusion detection. These findings underscore the significant role of deep learning in enhancing cybersecurity by enabling faster detection and response to cyber threats in cloud environments. The study also discusses the challenges and considerations of implementing honeypots in cloud infrastructures, such as privacy concerns and legal issues when dealing with third-party cloud service providers. The combination of honeypots with advanced machine learning techniques, including RNN and CNN, offers a promising direction for future research in cloud security.

Keywords: Honeypot, Intrusion Detection, RNN (Recurrent Neural Network), CNN Cybersecurity, Machine Learning, Network Traffic Analysis

1. 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 fullblown 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.

2. 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, [1]. The research community hasn't given cloud monitoring much attention despite how crucial it is for running cloud systems. An study of cloud monitoring is provided in this position paper. Discusses the primary drivers, fundamental ideas, and definitions, as well as highlighting unresolved problems in the field of study and potential avenues for cloud monitoring. A Review of the Security Framework for a Cloud Computing Environment [2]. Cloud computing has developed into a significant platform upon which businesses can construct their infrastructures. Companies who are considering utilising cloud-based systems will need to thoroughly re-evaluate both their current security measures and the features unique to the cloud in order to successful solution provider. The goal of the study, which the literature already in existence, is to specify a methodology of cloud providers that will safeguard users' data, which is extremely important information. Environments for Cloud Security Threats [3]. By providing service users with constant, practical, and on demand service network access to a shared pool of reconfigurable computer resources is called cloud computing. The cloud security is a new area of study, and this paper discusses cloud computing security issues based on an analysis of cloud security issues and technical cloud computing components. Cloud-based IDS based on virtual hosts [4]. Internet- or intranet-based cloud computing allows for the provisioning of infrastructure, data, and applications in response to demand. Due to the vast amounts of resources that are available in the cloud, its security has suffered a significant breach. The two main concerns are theft and loss of data. This study introduces a virtual host-based IDS and cloud intrusion detection data sets (CIDD). The attack signatures in CIDD are manually created and graded using a widely used vulnerability scoring system. They are based on ports that have been opened in the cloud for communications. The method utilised for extracting rules from existing datasets is known as a genetic algorithm. By using genetic operations, a sizable set of rules can be developed for intrusion detection. A cloud-based integrated intrusion handling called IDPS [5]. IDSs, or intrusion detection systems, are made to handle particular kinds of threats. It is obvious that no one method can provide assurance against future threats. Consequently, there is a need for an integrated system that can offer reliable protection against a wide range of threats. However, effectively detect and stop malicious traffic and activities, technology that empowers the network and its hosts to protect themselves with some amount of intelligence is desperately needed. In terms of security and privacy, this study focuses on contemporary IDS implementations in cloud computing environments. The IDPS, which combines both IDS and IPS into a single mechanism, is the model that is proposed in this research as being effective and efficient. Anomaly Detection and Signature Detection, two techniques that can cooperate to find a variety of threats and prevent them using the capabilities of IPS, are also integrated into the mechanism.

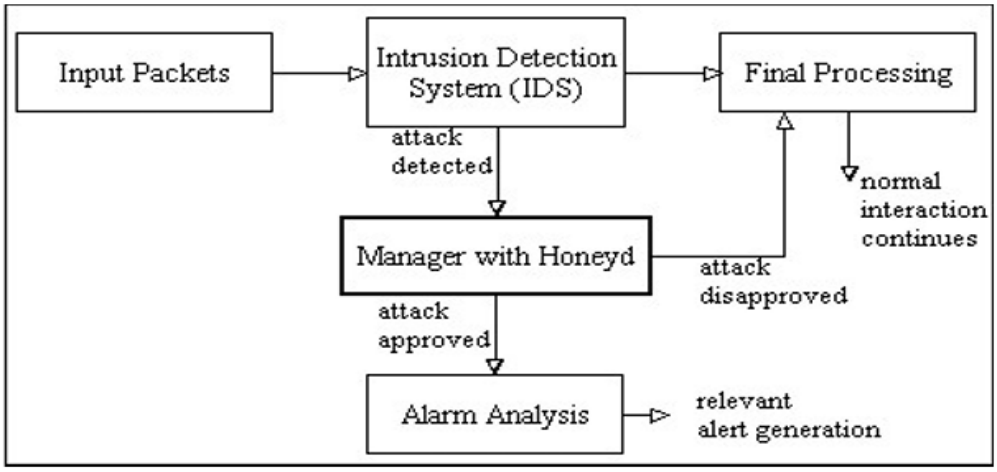
International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

3. METHODOLOGY

Attacks can target a system in a variety of ways and then take use of the known weaknesses in computer systems. In actuality, an attack results in the loss and disclosure of private data and sensitive information kept on the computer. Fig 1 shows the Architectural Design of Proposed Framework. In addition to traditional traffic profiling, the integrated model also incorporates signature matching to improve attack detection. In addition, the system deploys Intrusion Detection System in the virtual machine and virtual network to monitor system operations in addition to observing network packet traffic to filter malicious packets arriving from dubious sources. Since all data will pass through the Honeypot server, configured with firewall settings. A honeypot monitoring and alerting device. It is a network location that resembles an isolated area within the network. For hackers and attackers, it contains information that is incredibly useful. For hackers and attackers, the information contained in the honeypot is extremely useful. The innovative method of data and resource protection in Cloud environment with Honeypot is proposed in this work. It is founded on the effective use of intrusion detection systems throughout the Cloud computing infrastructure.

Client:

Client is a user who communicates to the server through IDS system. User can login his user id and password provided by server and do transactions like file upload and download.



Intrusion Detection System

By invaders' route, such as failed access trails, intrusion detection technology generally aids in identifying the unauthorised intrusions from both outside and inside of local network. The following components make up a typical IDS: an event generator, an event analyser, response units, and event databases. The pieces communicate using GIDOs (Generalised Intrusion Detection Objects) to share data. The definition of message is known as GIDO, and its encoded information can either be a single event that occurred at a given time, a conclusion about a series of occurrences, or an instruction to perform an action. Each part might be implemented as a single process on a computer, or might be a collection of many processes on a number of computers. The event generator gathers events from data outside of the intrusion detection system, creates events depending on the traffic therein, and then transfers them to the other elements in GIDO format.

C. Server Server holds the data provided by client. Server generates username and password for new user and sends it through email to client.

D. Honeypot This solution can prevent many poor choices made by IDS by utilising the honeypot scheme. In this system, IDS detected worrisome opponents will be forwarded to a honeypot network for a closer examination. The connection will be directed to the original destination carry on the earlier

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

interaction if it turns out that the alarm decision agent's IDS was incorrect as a consequence of this examination. The user is unaware of this action.

E. Client Validation When a client is blocked by IDS due to its suspicious behaviour, honeypot generates a verification code for client and sends it by email. The client has to authenticate itself using the verification code and continue with the services provided by server.

4. RESULTS AND DISCUSSION

The three components that make up the implemented project are the node, intrusion, and server modules. You can access all three modules by executing the main.java file. The user login form is a component of the node module. The user's credentials can be used to log in. In this study, we use a honeynet to collect and analyze potentially malicious network data, and we also provide various tools to aid in our investigation. Our design includes a web interface for tracking data collecting and a firewall for controlling outgoing connections from a potentially compromised honeypot. One low-cost tactic that medium-sized businesses often use to reap the benefits of a secure and sanitary compromise is utilizing a high-interaction honeypot host.

Ransomware Attack Detection using Honeypot Machine Learning

Ransomware encrypts the files of those who get infected with it. In order to get access to the data again, the hacker will ask the victim to pay a ransom. Ransomware can infiltrate a computer through multiple entry points. One of the most common methods of delivery is phishing, in which the spam arrives in an email with an attachment that looks like a file the recipient should trust. If they include social engineering tactics that trick users into giving them administrator access, they can take over the victim's computer once they've accessed and downloaded them. More malicious ransomware, like Not Petya, uses vulnerabilities to infect computers without tricking users. The ransomware attackers use a variety of techniques to choose which businesses to target. The timing can be a factor; for instance, hackers may target universities due to their broad user base and smaller security teams, which makes it easier to break their defenses. Hackers use honeypots, which are network-attached systems, as a trap to find and study the methods and types of assaults they use. In its role as a potential internet target, it notifies the guards of any intrusion attempts to the data system. Honeypots are most commonly used by large corporations and organizations who are concerned with cyber security. The many forms of attacks used by cybercriminals and attackers can be better understood with its help, according to cyber security researchers.

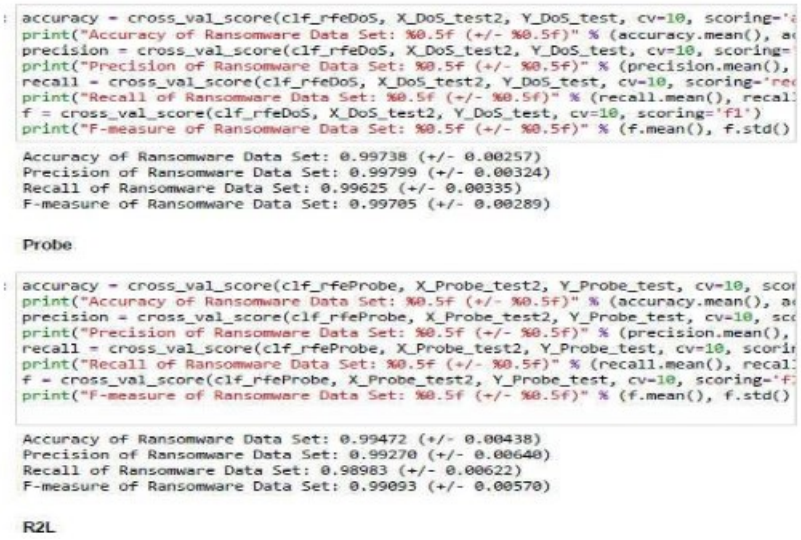


Figure: Accuracy, Precision, Recall Results for Machine Learning Algorithm.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

SVM

```
from sklearn.svm import SVC

clf_SVM_DoS=SVC(kernel='linear', C=1.0, random_state=0)
clf_SVM_Probe=SVC(kernel='linear', C=1.0, random_state=0)
clf_SVM_R2L=SVC(kernel='linear', C=1.0, random_state=0)
clf_SVM_U2R=SVC(kernel='linear', C=1.0, random_state=0)

clf_SVM_DoS.fit(X_DoS, Y_DoS.astype(int))
clf_SVM_Probe.fit(X_Probe, Y_Probe.astype(int))
clf_SVM_R2L.fit(X_R2L, Y_R2L.astype(int))
clf_SVM_U2R.fit(X_U2R, Y_U2R.astype(int))
```

```
SVC(kernel='linear', random_state=0)
```

Figure: Using SVM Classifier in Honeypot.

```
accuracy = cross_val_score(clf_voting_U2R, X_U2R_test, Y_U2R_test, cv=10, scoring
print("Accuracy of Ransomware Data Set: %0.5f (+/- %0.5f)" % (accuracy.mean(), ac
precision = cross_val_score(clf_voting_U2R, X_U2R_test, Y_U2R_test, cv=10, scorir
print("Precision of Ransomware Data Set: %0.5f (+/- %0.5f)" % (precision.mean(),
recall = cross_val_score(clf_voting_U2R, X_U2R_test, Y_U2R_test, cv=10, scoring='
print("Recall of Ransomware Data Set: %0.5f (+/- %0.5f)" % (recall.mean(), recall
f = cross_val_score(clf_voting_U2R, X_U2R_test, Y_U2R_test, cv=10, scoring='f1_ma
print("F-measure of Ransomware Data Set: %0.5f (+/- %0.5f)" % (f.mean(), f.std()
```

```
Accuracy of Ransomware Data Set: 0.99755 (+/- 0.00228)
Precision of Ransomware Data Set: 0.93843 (+/- 0.12993)
Recall of Ransomware Data Set: 0.87335 (+/- 0.13280)
F-measure of Ransomware Data Set: 0.89369 (+/- 0.11933)
```

Figure: accuracy, precision, Recall, F-measure

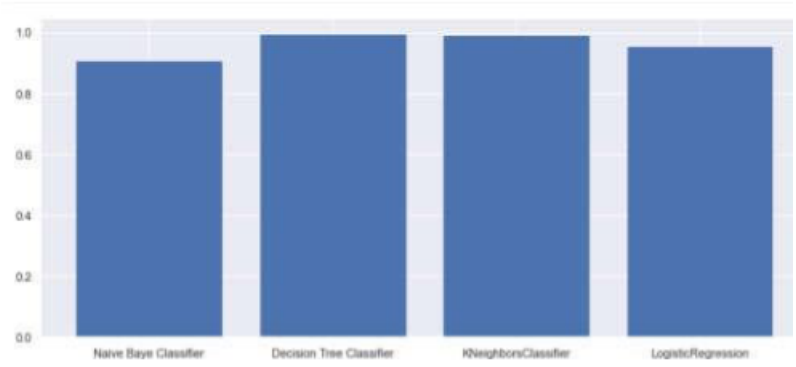


Figure: Comparison using Different Machine learning Algorithms

CONCLUSION

Production systems are somewhat protected by the proposed hybrid honeypot architecture approach. This is achieved by reducing the likelihood of hacker activity and attacks on our production systems. It does this by implementing network lure systems, which fool the hacker into thinking the honey systems are real systems by hiding information about them, their status, and even their fingerprints. To accomplish our objective, we need the redirection capabilities; otherwise, the production system would be left vulnerable to direct attacks that bypass the controlled honeypot. The proposed method restricts production honeypots to a passive function, recording various attacker actions for later data mining analysis by the system administrator. By analyzing the attacker's actions and limiting the variety of attacks through the use of a signature file or database, this could take a more proactive role in protecting my data.

References:

1. Dr. Mohammed Abdul Bari,Arul Raj Natraj Rajgopal, Dr.P. Swetha ,” Analysing AWSDevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution”, International Journal of Intelligent Systems and Applications in Engineering , JISAE, ISSN:2147-6799, Nov 2023, 12(4s), 519–526
2. Ijteba Sultana, Mohd Abdul Bari and Sanjay,” Impact of Intermediate per Nodes on the QoS Provision in Wireless Infrastructure less Networks”, Journal of Physics: Conference Series, Conf. Ser. 1998 012029 , CONSILIO Aug 2021
3. Mohammed Rahmat Ali, Digital Forensics and Artificial Intelligence ...A Study, International Journal of Innovative Science and Research Technology, ISSN:2456-2165, Volume: 5 Issue:12.
4. Mohammed Rahmat Ali, Usage of Technology in Small and Medium Scale Business, International Journal of Advanced Research in Science & Technology (IJARST), ISSN:2581-9429, Volume: 7 Issue:1, July 2020.
5. Mohammed Rahmat Ali, Internet of Things (IOT) Basics - An Introduction to the New Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-32-36, Volume: 5 Issue: 10
6. Mohammed Rahmat Ali, Internet of things (IOT) and information retrieval: an introduction, International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume: 7 Issue: 4, October 2017.