# Detection and Notification of Zero-Day Attack to prevent CyberCrime

N Afnan
Department of Computer Science
And Engineering
Cambridge Institute of Technology
K.R.Puram,Bangalore-560036,India.
afnan22.cse@cambridge.edu.in

Mohammed Usman Shaikh
Department of Computer Science
And Engineering
Cambridge Institute of Technology
K.R.Puram,Bangalore-560036,India.
usman.21cse@cambridge.edu.in

N S Umer
Department of Computer Science
And Engineering
Cambridge Institute of Technology
K.R.Puram,Bangalore-560036,India.
umer.21cse@cambridge.edu.in

Prof. J Sharon Christina
Department of Computer Science
And Engineering
Assistant Professor
Cambridge Institute of Technology
Bangalore
sharon.cse@cambridge.edu.in

**Abstract-** Network intrusion detection systems, often known as NIDS, are essential for protecting networks from many types of cyberattacks. However, because attacks are constantly changing, it can be difficult for traditional NIDS to identify complex incursions. The present study suggests integrating honeypots, deceptive network resources intended to entice attackers within a cloud computing environment to enhance the capabilities of network intrusion detection systems. Hosting honeypots on the cloud is a great concept because cloud computing provides scalable infrastructure and flexible resource allocation.

## I. Introduction

Network intrusion detection systems, often known as NIDS, are essential for protecting networks from many types of cyberattacks. However, because attacks are constantly changing, it can be difficult for traditional NIDS to identify complex incursions. The present study suggests integrating honeypots— deceptive network resources intended to entice attackers—within a cloud computing environment to enhance the capabilities of network intrusion detection systems. Hosting honeypots on the cloud is a great concept because cloud computing provides scalable infrastructure and flexible resource allocation.

## II. Problem Definition

One of the biggest challenges in Network in flow Security is today is the lack of coordination between different service providers. It may be as approaches such as suricata, zeek, filebeat, and in elastisearch, kibana, open canary pot. This allow section outlines,as architecture, components.

with The NIDS architecture is designed to be modular, scalable, and adaptable to diverse network environments. At its core, the system comprises Suricata and Zeek, two powerful network security monitoring tools known for their flexibility and performance. Suricata functions as the primary intrusion detection engine, capable of inspecting network traffic in real- time and detecting a wide range of threats based on signature-based and anomaly- based detection techniques. Zeek complements Suricata by providing detailed network traffic analysis and protocol extraction, enabling the extraction of rich metadata for threat intelligence purposes.

## III. Literature Review

Many studies highlight the growing role of digital solutions in (NIDS). Research on intrusion and Detection systems emphasizes the importance of integrating cyber security Overall, the proposed NIDS system leverages a combination of open-source tools and innovative methodologies to enhance network security posture, detect emerging threats, and enable proactive threat mitigation and incident response. By integrating signature-based detection, anomaly detection, log management, and deception technologies, the proposed system offers.
[1] Neha Sharma ,DR. Kavitha “Performance Study of Snort and Suricata for Intrusion Detection System”.

**Advantages:** The performance study of Snort and Suricata for Intrusion Detection Systems (IDS) reveals several advantages for both.

**Disadvantages:** Snort's disadvantages include high a

false positive rates, which can lead to unnecessary alerts.

[2] Zeeshan Ahmed, Adnan Shahid Khan "A Systematic Study of Machine Learning and Deep Learning Approaches".

**Advantages:** Machine learning algorithms such as Support Vector Machines (SVM), Random Forest.

**Disadvantages:** One major limitation is the requirement for large amounts of labeled training data, which can be time-consuming and expensive to obtain.

[3] D.A. Fernandes, L.F. Soares, J.V. Gomes Intrusion Detection System for Cloud Computing.

**Advantages**: IDS can detect and prevent intrusions in real-time, reducing the risk of data breaches and cyber attacks.

**Disadvantages:** Despite its benefits, an Intrusion Detection System (IDS) for Cloud Computing also has some disadvantages.

**[5]** Another popular survey by Kabiri and Ghorbani presented trends in IDS and also analyzed some problems regarding intrusion detection.

**Advantages:** The presented trends in Intrusion Detection Systems (IDS) offer several advantages, including improved threat detection and incident response capabilities.

**Disadvantages:** The reliance on machine learning and AI algorithms can lead to false positives and negatives, and the need for continuous training and updating of models.

## IV. Key Components

**Suricata:** Suricata serves as the most in applicable for security threats. Leveraging its support for multi-threading and high-speed packet processing, Suricata offers real-time intrusion detection capabilities, including signature-based detection, protocol analysis, and file extraction.

**Zeek**: Formerly known as Bro, Zeek operates alongside Suricata to provide network visibility and protocol analysis. Zeek passively monitors network traffic, extracting high-level semantic information from packet headers and payloads. By analyzing network protocols and behaviors, Zeek can detect a wide range of anomalies and suspicious activities that may evade traditional signature-based detection mechanisms.

**File Beat**: File beat is utilized for log collection and forwarding, enabling the centralization of security event data from various sources. By collecting logs generated by Suricata, Zeek, and other network devices, File beat ensures that all relevant security events are captured and forwarded to the backend datastore for analysis and correlation.

**Elasticsearch**: Elasticsearch serves as the backend datastore, storing and indexing security event data for rapid retrieval and analysis. With its distributed and scalable architecture, Elasticsearch enables efficient storage and querying of large volumes of security logs, facilitating real-time monitoring and forensic analysis.

**Kibana**: Kibana complement are Elasticsearch by defnation

user-friendly interface for visualizing and querying security data. Security analysts can leverage Kibana's interactive dashboards and visualization tools to gain insights into network traffic patterns, detect anomalies, and investigate security incidents.

**Open Canary Honeypot:** Open Canary is deployed as a deception mechanism to detect and deceive attackers attempting to infiltrate the network. By emulating vulnerable services and systems, Open Canary lures attackers into engaging with decoy assets, providing valuable insights into their tactics, techniques, and procedures (TTPs).

## V. Features and Functionality

- Real-time intrusion detection Suricata and Zeek analyze network traffic in real-time, detecting and alerting security personnel to suspicious activities and potential security breaches.
- Network visibility and protocol analysis Zeek provides detailed network traffic analysis, extracting high-level semantic information from packet headers and payloads to identify anomalies and malicious behaviors.
- Log management and analysis: File beat collects and forwards security event logs to Elasticsearch, where they are indexed and stored for further analysis and correlation.
- Visualization and reporting: Kibana offers interactive dashboards and visualization

## VII. Results and Outputs

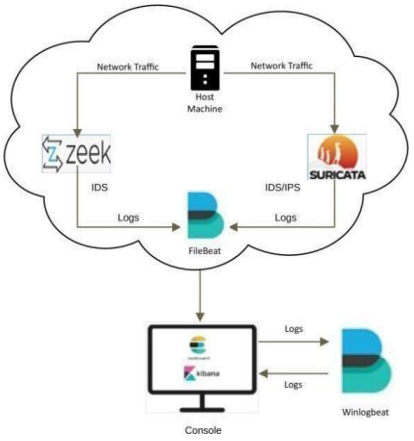


Fig 1. Architecture Diagram

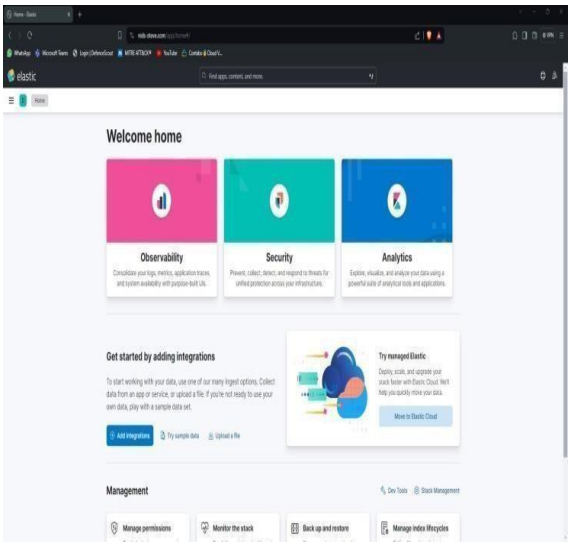


Fig 2. Home Page

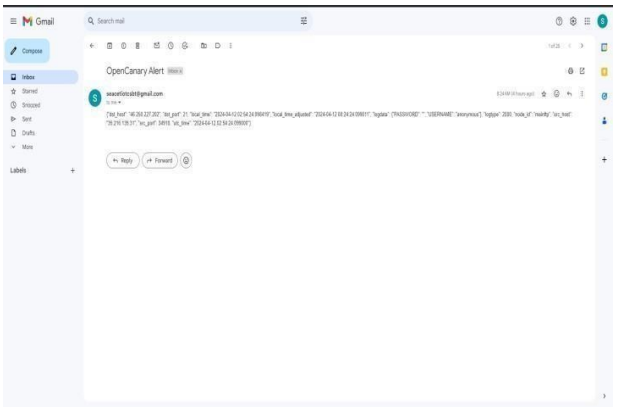


Fig 3. Emails generated by Honey pot

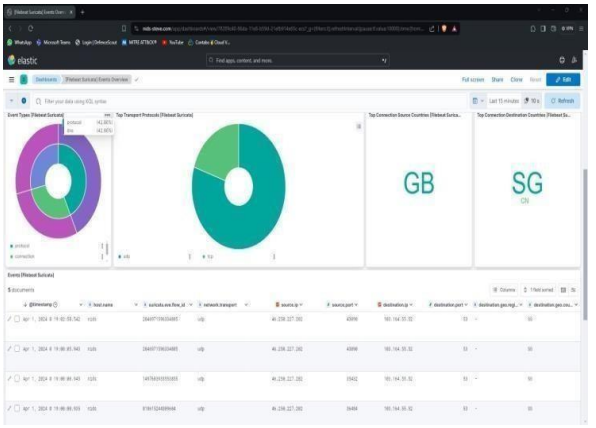


Fig 4. Suricata Dashboard

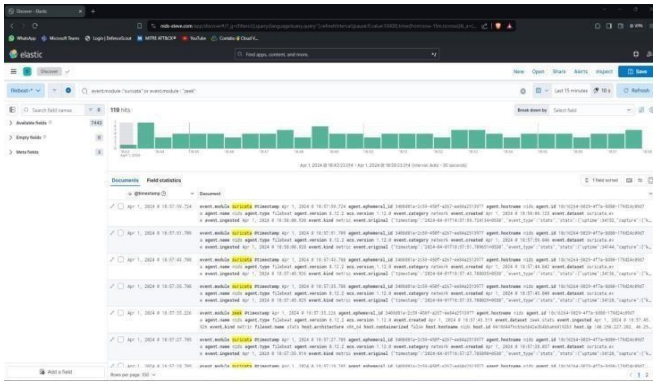

Fig 5. Discover Page

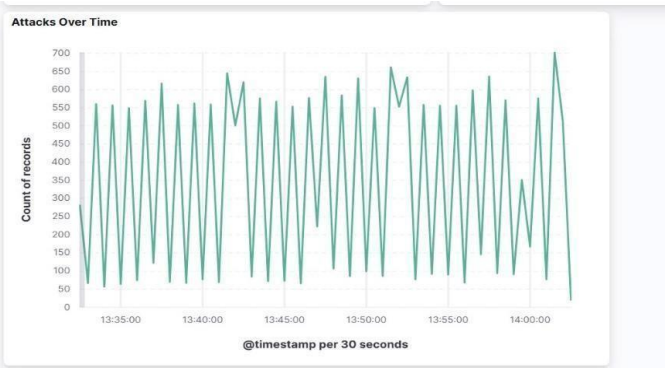


Fig 6. Attacks over time


Fig 8. Destination Locations

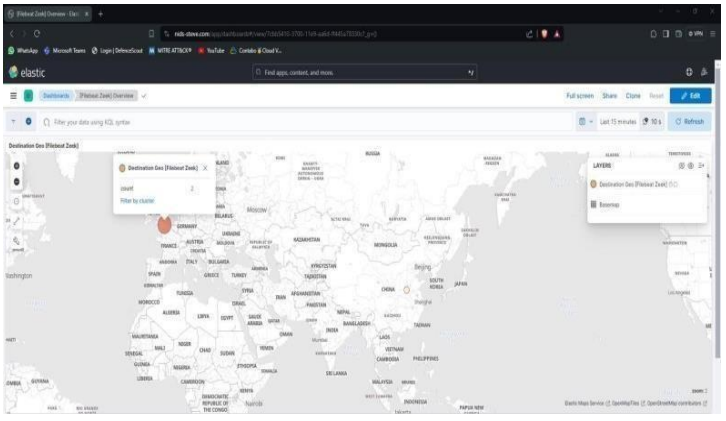

Fig 9. Zeek Dashboard

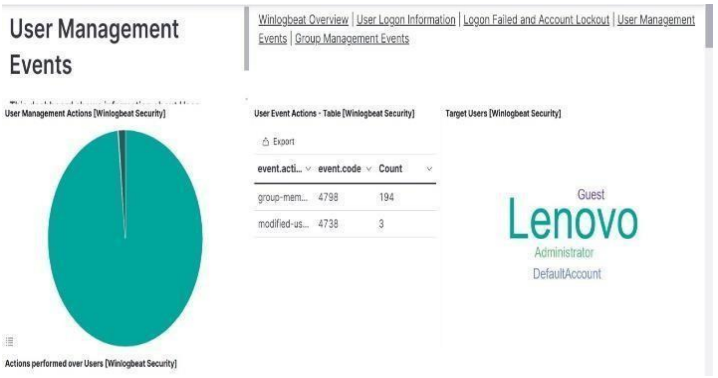


Fig 10. User management Events

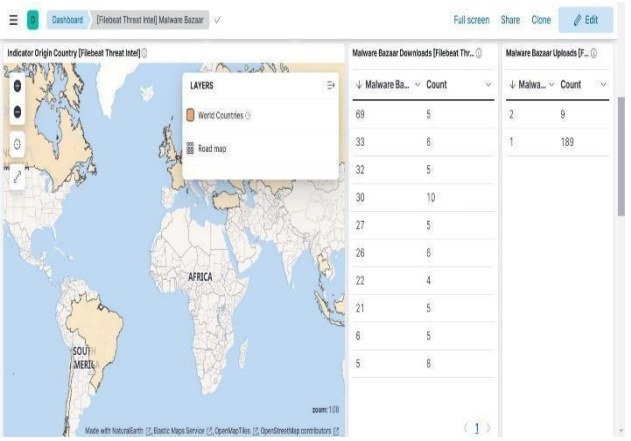


Fig 11. Dashboard of threats

## VIII. Conclusion

This study demonstrates the usefulness of an NIDS in a small- to medium-sized business (SME) network setting. Using Suricata, Zeek, File beat, and the Elastic, the NIDS effectively identified and addressed a range of security risks, such as port scans, brute force assaults, and suspicious outgoing traffic. The organization's network security is improved by the capacity to perform post-event analysis and obtain real time alerts via Kibana, protecting its vital Open Canary honeypot is deployed to provide the in company with more information about potential as the dangers and attacker behaviors. By luring potential and attackers to engage with it, the Open Canary honeypot serves as a decoy and draws their focus away from the important assets. When the security team monitors of and examines the attacker's tactics, methods, and the procedures (TTPs), any interaction with the honeypot sets off alarms. Moreover, an extensive picture of the the threat landscape may be obtained by correlating information gathered from the Open Canary honeypot with the warnings produced by the NIDS. The firm is able to recognize new threats, adjust security procedures, and enhance defenses over time thanks to this integrated strategy.the NIDS enables the SME to keep its network resources and client data safe and secure while swiftly responding to security problems The SME network environment's security posture is further strengthened by the addition of an Open Canary honeypot. Alongside the NIDS, the Open Canary honeypot is deployed to provide the company with more information about potential dangers and attacker behaviors. By luring potential attackers to the engage with it, the Open Canary honeypot serves as a decoy and draws their focus away from important assets. When the security team monitors and examines the attacker's tactics, methods, and procedures (TTPs), any interaction with the honeypot sets off alarms.Moreover, an extensive picture of the threat landscape may be obtained by correlating the information gathered from the Open Canary honeypot with the warnings produced by the NIDS. The firm is able to recognize new threats, adjust security procedures, and enhance defenses over time thanks to this integrated strategy. Through the integration of the NIDS's capabilities with the Open Canary honeypot's insights, the SMEs may enhance their resilience against cyberattacks by proactively safeguarding against known and new threat.

## IX. References

[1] Neha V Sharma , Kavita, Gaurav Aggarwal and Saurabh Sharma ,Performance Study of Snort and Suricata for Intrusion Detection System‘‘ Department of Information Technology, Manipal University Jaipur, Jaipur-Ajmer Express Highway, Dehli Kalan, Near GVK Toll Plaza, Jaipur, Rajasthan 303007 India 2Amity School of Hospitality, Amity University Rajasthan, SP-1 Kant Kalwar, NH11C, RIICO Industrial Area, Jaipur, Rajasthan 303007 India.

[2] Ahmad, Zeeshan & Shahid Khan, Adnan & Shiang, Cheah & Ahmad, Farhan. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies. 32. 10.1002/ett.4150.

[3] Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande Intrusion Detection System for Cloud Computing‖ International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012 ISSN2277-8616.

[4] M.R. Amal & P. Venkatesh, Review of Cyber Attack Detection: Honeypot System ‘‘Web logy, Volume 19, Number 1, January, 2022.

[5] Mr. Saurabh Alva, Mr. Rahul Madhyan, Mr. Anoop Madan Implementation of Honeypot ‘‘ International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869 (O) 2454-4698 (P),Volume-3, Issue-8, August 2015.

[6] P.S. Negi, A. Garg and R. Lal, "Intrusion Detection, Prevention, using Honeypot Network for Cloud Security," 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2020, pp. 129-132, doi: 10.1109/Confluence47617.2020.9057961.

[7] M. Bishop, __Trends in academic research: Vulnerabilities analysis and intrusion detection,‘‘ Compute. Secure., vol. 21, no. 7, pp. , Nov. 2002.

[8] Bikrant Gautam, Network Intrusion Detection System And Analysis, Security and Cryptographic Protocol 606 ,2015,SCSU.

[9] S. Kumar, S. Gupta and S. Arora, "Research Trends in Network- Based Intrusion Detection Systems: A Review," in IEEE Access, vol. 9, pp. 157761-157779,2021,doi:10.1109/ACCESS.2021.312977.

[10] J. Liu, K. Xiao, L. Luo, Y. Li and L. Chen, "An intrusion detection system integrating network-level intrusion detection and host-level Intrusion detection," 2020 IEEE 20th International Conference on Software Quality, Reliability and Security (QRS), Macau, China, 2020,pp.122-doi:10.1109/QRS51102.2020.00028.

[11] H. Wang, J. Gu, and S. Wang, "An effective intrusion detection frame-work based on SVM with feature augmentation," Known.- Based Syst., vol. 136, pp. 130-139, Nov. 2017.

[12] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques : Existing solutions and latest technological trends," Compute. Netw., vol. 51, no. 12, pp. 3448-3470, Aug. 2007

[13] J. J. Treinen and R. Thuri mella,"A framework for the application of association rule mining in large intrusion detection infrastructures," in Proc. 9th Int. Conf. Recent Adv. Intrusion Detection,2006, pp. 1-18

[14]L. Tan and T. Sherwood, "A high throughput

string matching architecture for intrusion detection and prevention," in Proc. 32nd Int. Symp. Compute. Archit. (ISCA), vol. 33, 2005, pp. 112-122.

[15] G. Sourek and F. Zelezny, "Efficient extraction of network event types from Net Flows," Secure Communication .Net., vol. 2019, pp. 1- 18, Feb. 2019.

[16] M. Sazzadul Hoque, M. A. Mukit, and M. A. N. Bikas, "An implementation of intrusion detection system using genetic algorithm," 2012, arXiv: 1204.1336.

[17] S. X. Wu and W. Banzhaf, "Review: The use of computational intelligence in intrusion detection systems: A review," Appl. Soft Compute, vol. 10, no. 1, pp. 1-35, 2010.

[18] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified k-means for intrusion detection system," Expert Syst. Appl., vol. 67, pp. 296-303, Jan. 2017.

[19] H. Wang, J. Gu, and S. Wang, "An effective intrusion detection frame-work based on SVM with feature augmentation," Known. Based Syst., vol. 136, pp. 130-139,Nov.2017.

[20] G. Sourek and F. Zelezny, "Efficient extraction of network event types from Net Flows," Secure. Commun. Net., vol. 2019, pp. 1-18, Feb. 2019.

[21] L. C. Smith, "Citation analysis," Library Trends, vol. 30, no. 1, pp. 83-106, 1981.

[22] The Top List of Academic Search Engines, Paper pile, Cambridge, MA, USA, Jun.2021.[Online].

[23] List of Academic Databases and Search Engines, Wikimedia found, San Francisco, CA ,USA,Jun.2021.

[24] Microsoft Academic. Accessed: Dec 20,2020. [Online].Available: https://academic.microsoft.com.

[25] he Top List of Academic search Engines, Paperpile, Cambridge, MA, USA,Jun.2021.[Online].Available:https://paperpile.com/g/academic-search-engines.