Next-Generation Network Intrusion Detection and Prevention System

#1 J.KUMARI, #2 G. SATHWIKA
#1 ASSISTANT PROFESSOR, #2 MCA SCHOLAR
DEPARTMENT OF MASTER OF COMPUTER APPICATIONS
QIS COLLEGE OF ENGINEERING & TECHNOLOGY
VENGAMUKKALAPALEM(V), ONGOLE, PRAKASAM DIST., ANDHRA PRADESH

ABSTRACT:

This study outlines a novel method for assisting clinicians in making retinitis pigmentosa diagnoses, beginning with an examination of pediatric patients' pupil responses to chromatic light stimuli. The system's purpose was to clean theOne of the most significant topics that has garnered a lot of research and development attention in recent years is cloud security. Attackers can specifically investigate cloud system vulnerabilities and hack virtual machines in order to launch additional extensive Distributed Denial-of-Service (DDoS) attacks. Early-stage tactics including multi-step exploitation, low frequency vulnerability scanning, and compromising identified weak virtual machines as zombies are typically used in DDoS attacks. Once the compromised zombies are compromised, DDoS attacks are typically launched. It is quite challenging to identify zombie exploration assaults in cloud systems, particularly Infrastructure-as-a-Service (IaaS) clouds. This is due to the possibility of cloud users installing susceptible software on their virtual computers. We propose NICE, a multi-phase distributed vulnerability detection, measurement, and countermeasure selection mechanism based on attack graph-based analytical models and reconfigurable virtual network-based countermeasures, to stop vulnerable virtual machines from being compromised in the cloud. To greatly enhance attack detection and lessen attack repercussions, the suggested architecture builds a monitor and control plane over distributed programmable virtual switches using Open Flow network programming APIs. The effectiveness and efficiency of the suggested solution are shown by the system and security assessments.using a machine learning technique based on an ensemble model of two fine-tuned SVMs to identify tefacts, extract features, and aid in the diagnosis of RP. Both the left and right eyes' performances were assessed using a leave-one-out cross-validation, which was also utilized to determine the optimal set of SVM internal parameters. In order to enhance the total sensitivity of the CDSS, the class given to each eye was ultimately merged using an OR-like strategy; the ensemble system obtained 84.6% accuracy, 93.7% sensitivity, and 78.6% specificity. Given the limited quantity of data available for this work, additional testing with a bigger data pool is necessary to validate the system's performance. The testing of the same strategy with several devices is part of the future scope.

I. INTRODUCTION

Information security as it relates to computers and networks is called computer security, sometimes referred to as cyber security or IT security. The field encompasses all procedures and systems that guard computer-based tools, data, and services from illegal or unintentional access, alteration, or destruction. Protection against unforeseen circumstances and natural calamities is another aspect of computer security. Otherwise, the term "security" or "computer security" in the context of the computer business refers to methods of making sure that information stored on a computer cannot be viewed or compromised by unauthorized individuals. Passwords and data encryption are used in the majority of computer security procedures. Transforming data into an incoherent format without a deciphering method is known as data encryption. A password is a coded word or phrase that allows a user to access a certain system or software.

Diagram clearly explain the about the secure computing

Technical measures like login passwords, anti-virus are essential. (More about those below) However, a secure physical space is the first and more important line of defense. Is the place you keep your workplace computer secure enough to prevent theft or access to it while you are away? While the Security Department provides coverage across the Medical center, it only takes seconds to steal a computer, particularly a portable device like a laptop or a PDA. A computer should be secured like any other valuable possession when you are not present. Human threats are not the only concern. Computers can be compromised by environmental mishaps (e.g., water, coffee) or physical trauma. Make sure the physical location of your computer takes account of those risks as well. The University's networks and shared information systems are protected in part by login credentials (user-IDs and passwords). Access passwords are also an essential protection for personal computers in most circumstances. Offices are usually open and shared spaces, so physical access to computers cannot be completely controlled. To protect your computer, you should consider setting passwords for particularly sensitive applications resident on the computer (e.g., data analysis software), if the software provides that capability. Because we deal with all facets of clinical, research, educational and administrative data here on the medical campus, it is important to do everything possible to minimize exposure of data to unauthorized individuals. Up-to-date, properly configured anti-virus software is essential. While we have server-side anti-virus software on our network computers, you still need it on the client side (your computer). Anti-virus products inspect files

on your computer and in email. Firewall software and hardware monitor communications between your computer and the outside world. That is essential for any networked computer.

It is critical to keep software up to date, especially the operating system, anti-virus and anti-spyware, email and browser software. The newest versions will contain fixes for discovered vulnerabilities. Almost all anti-virus have automatic update features (including SAV). Keeping the "signatures" (digital patterns) of malicious software detectors up-to-date is essential for these products to be effective.

Even if you take all these security steps, bad things can still happen. Be prepared for the worst by making backup copies of critical data, and keeping those backup copies in a separate, secure location. For example, use supplemental hard drives, CDs/DVDs, or flash drives to store critical, hard-to-replace data.

II. RELATED WORKS

The evolution of cyber threats has necessitated the advancement of network security systems beyond traditional intrusion detection systems (IDS) and intrusion prevention systems (IPS). Recent works have explored the integration of machine learning, deep learning, cloud computing, and software-defined networking (SDN) in developing Next-Generation Intrusion Detection and Prevention Systems (NG-NIDPS).

1. Signature-Based vs. Anomaly-Based IDS
   Traditional IDS approaches like Snort and Suricata rely heavily on signature-based detection. However, these are limited in identifying zero-day and evolving threats. To overcome this, researchers like Garcia-Teodoro et al. (2009) introduced hybrid models combining anomaly and misuse detection, improving adaptability and reducing false positives.
2. Machine Learning Techniques
   The use of ML techniques such as Random Forest, SVM, and k-NN has been widely studied. Kumar et al. (2020) implemented a machine learning-based IDS using the NSL-KDD dataset, showing improved detection rates compared to classical models. However, these models often suffer from high computational overhead in real-time environments.
3. Deep Learning Approaches
   Deep learning models, particularly CNNs and RNNs, have shown promising results in feature extraction and traffic classification. Shone et al. (2018) proposed a deep autoencoder-based model for intrusion detection, effectively capturing complex patterns in traffic data.
4. Software Defined Networking (SDN)
   SDN has enabled dynamic traffic control and improved monitoring. Yoon et al. (2019) developed an SDN-based intrusion prevention framework that detects and blocks malicious traffic in real time,

offering centralized control and fast response.

5. Cloud and Edge-Based NIDPS Researchers have also explored cloud-based NIDPS to address scalability and processing limitations. Zhao et al. (2021) proposed an edge-assisted cloud IDS architecture, reducing latency and enabling faster threat detection at the network edge.
6. Hybrid Models Hybrid detection systems combining statistical, ML, and rule-based methods are becoming common. Mehmood et al. (2020) introduced a hybrid IDS using decision trees and neural networks, significantly lowering false positives.
7. Datasets and Benchmarks Benchmark datasets like NSL-KDD, CICIDS2017, and UNSW-NB15 are commonly used for evaluating NIDPS performance. However, Ring et al. (2019) pointed out the limitations of synthetic datasets and stressed the need for real-world traffic data for effective evaluation.
8. Explainability and Trust Recent works focus on explainable AI (XAI) to make NIDPS decisions more transparent. Doshi-Velez & Kim (2017) emphasized the importance of interpretable models in security applications, helping administrators understand and trust the system's actions.

III. SYSTEM ANALYSIS

Existing System

Cloud users can install vulnerable software on their VMs, which essentially contributes to loopholes in cloud security. The challenge is to establish an effective vulnerability/attack detection and response system for accurately identifying attacks and minimizing the impact of security breach to cloud users. In a cloud system where the infrastructure is shared by potentially millions of users, abuse and nefarious use of the shared infrastructure benefits attackers to exploit vulnerabilities of the cloud and use its resource to deploy attacks in more efficient ways. Such attacks are more effective in the cloud environment since cloud users usually share computing resources, e.g., being connected through the same switch, sharing with the same data storage and file systems, even with potential attackers. The similar setup for VMs in the cloud, e.g., virtualization techniques, VM OS, installed vulnerable software, networking, etc., attracts attackers to compromise multiple VMs.

Disadvantages

1. No detection and prevention framework in a virtual networking environment.
2. Not accuracy in the attack detection from attackers.

Proposed System:

In this article, we propose NICE (Network Intrusion detection and Countermeasure selection in virtual network systems) to

establish a defense-in-depth intrusion detection framework. For better attack detection, NICE incorporates attack graph analytical procedures into the intrusion detection processes. We must note that the design of NICE does not intend to improve any of the existing intrusion detection algorithms; indeed, NICE employs a reconfigurable virtual networking approach to detect and counter the attempts to compromise VMs, thus preventing zombie VMs.

Advantages:

- We devise NICE, a new multi-phase distributed network intrusion detection and prevention framework in a virtual networking environment that captures and inspects suspicious cloud traffic without interrupting users' applications and cloud services.
- NICE incorporates a software switching solution to quarantine and inspect suspicious VMs for further investigation and protection. Through programmable network approaches, NICE can improve the attack detection probability and improve the resiliency to VM exploitation attack without interrupting existing normal cloud services.
- NICE employs a novel attack graph approach for attack detection and prevention by correlating attack behavior and also suggests effective countermeasures.
- NICE optimizes the implementation on cloud servers to minimize resource consumption. Our study shows that NICE consumes less computational overhead compared to proxy-based network intrusion detection solutions.

IV.**IMPLEMENTATION**

Modules

Nice-A

The NICE-A is a Network-based Intrusion Detection System (NIDS) agent installed in each cloud server. It scans the traffic going through the bridges that control all the traffic among VMs and in/out from the physical cloud servers. It will sniff a mirroring port on each virtual bridge in the Open vSwitch. Each bridge forms an isolated subnet in the virtual network and connects to all related VMs. The traffic generated from the VMs on the mirrored software bridge will be mirrored to a specific port on a specific bridge using SPAN, RSPAN, or ERSPAN methods. It's more efficient to scan the traffic in cloud server since all traffic in the cloud server needs go through it; however our design is independent to the installed VM. The false alarm rate could be reduced through our architecture design.

VM Profiling

Virtual machines in the cloud can be profiled to get precise information about their state, services running, open ports, etc. One major factor that counts towards a VM profile is its connectivity with other VMs.

Also required is the knowledge of services running on a VM so as to verify the authenticity of alerts pertaining to that VM. An attacker can use port scanning program to perform an intense examination of the network to look for open ports on any VM. So information about any open ports on a VM and the history of opened ports plays a significant role in determining how vulnerable the VM is. All these factors combined will form the VM profile. VM profiles are maintained in a database and contain comprehensive information about vulnerabilities, alert and traffic.

Attack Analyzer

The major functions of NICE system are performed by attack analyzer, which includes procedures such as attack graph construction and update, alert correlation and countermeasure selection. The process of constructing and utilizing the Scenario Attack Graph (SAG) consists of three phases: information gathering, attack graph construction, and potential exploit path analysis. With this information, attack paths can be modeled using SAG. The Attack Analyzer also handles alert correlation and analysis operations. This component has two major functions: (1) constructs Alert Correlation Graph (ACG), (2) provides threat information and appropriate countermeasures to network controller for virtual network reconfiguration. NICE attack graph is constructed based on the following information: Cloud system information, Virtual network topology and configuration information, Vulnerability information

Network Controller

The network controller is a key component to support the programmable networking capability to realize the virtual network reconfiguration. In NICE, we integrated the control functions for both OVS and OFS into the network controller that allows the cloud system to set security/filtering rules in an integrated and comprehensive manner. The network controller is responsible for collecting network information of current Open Flow network and provides input to the attack analyzer to construct attack graphs. In NICE, the network control also consults with the attack analyzer for the flow access control by setting up the filtering rules on the corresponding OVS and OFS. Network controller is also responsible for applying the countermeasure from attack analyzer. Based on *VM Security Index* and severity of an alert, countermeasures are selected by NICE and executed by the network controller.

Methodology

1. Data Collection

- Source: Network traffic is collected from routers, firewalls, switches, and IoT devices.
- Types of Data: Packet headers, flow data (NetFlow/sFlow), logs, and payload information.
- Tools: Wireshark, tcpdump, or custom packet sniffers integrated into the network.

2. Preprocessing

- Data Cleaning: Remove noise, irrelevant features, and corrupted packets.
- Normalization: Standardize data features to bring them into a similar range (e.g., Min-Max scaling).
- Feature Extraction: Use tools like PCA or information gain to select relevant features such as:
    - Source/Destination IP & Port
    - Protocol
    - Packet size
    - Flow duration
    - Number of bytes/packets sent/received

3. Detection Engine

- Hybrid Model Implementation:
    - Signature-Based Module: Matches traffic patterns with known attack signatures (e.g., Snort rules).
    - Anomaly-Based Module: Uses ML/DL algorithms to identify deviations from normal traffic.
- Machine Learning Models:
    - Random Forest, SVM, KNN for quick classification.
- Deep Learning Models:
    - CNN for spatial patterns in packet features.
    - LSTM for temporal behavior of traffic (sequence modeling).

4. SDN Integration (Optional for Dynamic Control)

- Controller Module: Communicates with switches/routers via OpenFlow to reroute or block traffic dynamically.
- Real-time Feedback Loop: Once a threat is detected, the SDN controller updates flow rules to mitigate the threat.

5. Threat Classification & Prioritization

- Multi-Class Labeling: Classify threats as DoS, DDoS, Botnet, Probe, Ransomware, etc.
- Threat Level Assessment: Assign severity scores based on frequency, affected nodes, and behavior pattern.
- Explainability Module (XAI): Use SHAP or LIME to provide interpretable decisions for alerts.

6. Prevention Mechanism

- Automatic Actions:
    - Alert administrators.
    - Drop malicious packets.
    - Block IP addresses or ports.
    - Isolate affected segments in the network.
- Manual Override: Interface for network administrators to approve or deny actions in critical environments.

7. Logging and Visualization

- Dashboard Interface:
    - Real-time visualization of network activity.

- Display detected threats, affected systems, and response actions.

- Log Management:
  - Store detected incident logs in a SIEM-compatible format for audit and compliance.

8. Model Training & Update

- Offline Training: Periodically retrain ML/DL models using updated datasets like CICIDS2017 or UNSW-NB15.
- Online Learning (Optional): Adaptive models that learn from new patterns during operation.
- Auto-Tuning: Use techniques like grid search or Bayesian optimization for hyperparameter tuning.

V. RESULTS AND DISCUSSION

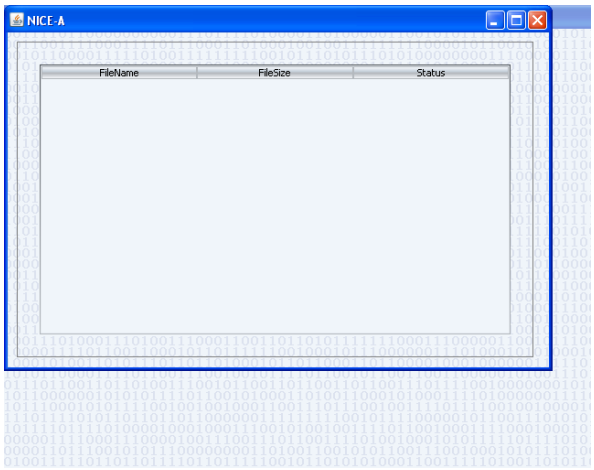

Fig 1

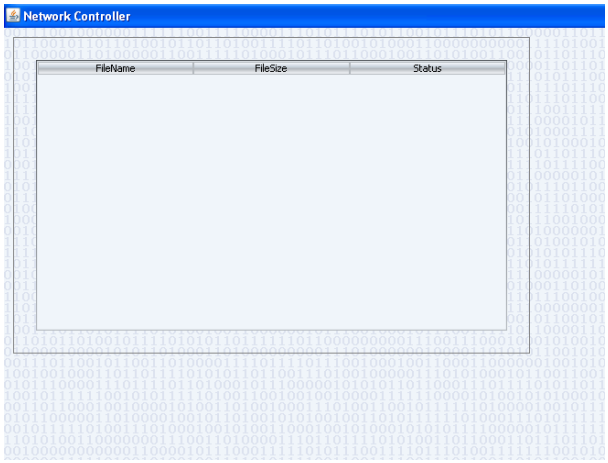

Fig 2

VI. FUTURE SCOPE AND CONCLUSION

NICE, which is intended to identify and lessen collaborative attacks in the cloud virtual networking environment, was introduced in this study. NICE performs attack detection and prediction using the attack graph concept. The suggested method looks into how to increase the detection accuracy and stop the victim exploitation stages of cooperative assaults by utilizing the programmability of software switch-based solutions. The system performance study proves that NICE is feasible and that the suggested solution can greatly lower the likelihood that both internal and external attackers will take advantage of and abuse the cloud system. NICE only looks into network intrusion detection systems to prevent zombie exploration attacks. It is necessary to cover the entire spectrum of IDS in the cloud system and integrate host-based IDS solutions to increase detection accuracy. This has to be looked upon in subsequent research. Furthermore, as stated in the paper, we will examine the

decentralized network control and attack analysis model based on current research in order to determine the scalability of the suggested NICE solution.

Future Enchancement

A number of future improvements could be taken into consideration in order to fortify and update the suggested network intrusion detection and prevention architecture. Advanced artificial intelligence and deep learning models, like recurrent neural networks (rnns) or convolutional neural networks (cnns), can be integrated to greatly enhance the system's detection capabilities of complex and yet undetected threats. As cloud computing gains popularity, the architecture should change to a cloud-native design that supports orchestration and containerization for increased scalability and flexibility. The system must also be improved to analyze encrypted communication using methods like ssl/tls fingerprinting and traffic pattern analysis without compromising privacy. While interaction with Soar (security orchestration, automation, and response) platforms can allow for real-time automated responses to threats, federated learning can provide privacy-preserving model updates over dispersed networks. The effectiveness of the system in thwarting contemporary cyberthreats will be further increased by extending support for industrial and IoT networks, enhancing visualization dashboards, and permitting threat intelligence sharing with international databases.

REFERENCES

[1] Coud Sercurity Alliance, “Top threats to cloud computing v1.0,” https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, March 2010.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia “A view of cloud computing,” *ACM Commun.*, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[3] B. Joshi, A. Vijayan, and B. Joshi, “Securing cloud computing environment against DDoS attacks,” *IEEE Int’l Conf. Computer Communication and Informatics (ICCCI ’12)*, Jan. 2012.

[4] H. Takabi, J. B. Joshi, and G. Ahn, “Security and privacy challenges in cloud computing environments,” *IEEE Security & Privacy*, vol. 8, no. 6, pp. 24–31, Dec. 2010.

[5] “Open vSwitch project,” http://openvswitch.org, May 2012.

[6] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker, “Detecting spam zombies by monitoring outgoing messages,” *IEEE Trans. Dependable and Secure Computing*, vol. 9, no. 2, pp. 198–210, Apr. 2012. IEEE TRANSACTIONS ON DEPEDABLE AND SECURE COMPUTING

[7] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, “BotHunter: detecting malware infection through IDS-driven dialog correlation,” *Proc. of 16th USENIX Security Symp. (SS ’07)*, pp. 12:1–12:16, Aug. 2007.

[8] G. Gu, J. Zhang, and W. Lee, “BotSniffer: detecting botnet command and control channels in network traffic,” *Proc. of 15th Ann. Network and Distributed Sytem Security Symp. (NDSS ’08)*, Fb. 2008.

[9] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," *Proc. IEEE Symp. on Security and Privacy*, 2002, pp. 273–284.
[10] "NuSMV: A new symbolic model checker," http://afrodite.itc.it: 1024/∼nusmv. Aug. 2012.
[11] S. H. Ahmadinejad, S. Jalili, and M. Abadi, "A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs," *Computer Networks*, vol. 55, no. 9, pp. 2221–2240, Jun. 2011.
[12] X. Ou, S. Govindavajhala, and A. W. Appel, "MulVAL: a logicbased network security analyzer," *Proc. of 14th USENIX Security Symp.*, pp. 113–128. 2005.
[13] R. Sadoddin and A. Ghorbani, "Alert correlation survey: framework and techniques," *Proc. ACM Int'l Conf. on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services (PST '06)*, pp. 37:1–37:10. 2006.
[14] L. Wang, A. Liu, and S. Jajodia, "Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts," *Computer Communications*, vol. 29, no. 15, pp. 2917–2933, Sep. 2006.
[15] S. Roschke, F. Cheng, and C. Meinel, "A new alert correlation algorithm based on attack graph," *Computational Intelligence in Security for Information Systems*, LNCS, vol. 6694, pp. 58–67. Springer, 2011.
[16] A. Roy, D. S. Kim, and K. Trivedi, "Scalable optimal countermeasure selection using implicit enumeration on attack countermeasure trees," *Proc. IEEE Int'l Conf. on Dependable Systems Networks (DSN '12)*, Jun. 2012.
[17] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic security risk management using bayesian attack graphs," *IEEE Trans. Dependable and Secure Computing*, vol. 9, no. 1, pp. 61–74, Feb. 2012.
[18] Open Networking Fundation, "Software-defined networking: The new norm for networks," *ONF White Paper*, Apr. 2012.

Authors Profile

Mrs. J.KUMARI is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. She earned MCA from Osmania University, Hyderabad, and her M.Tech in Computer Science and Engineering (CSE) from Jawaharlal Nehru Technological University, Kakinada (JNTUK). Her research interests include Machine Learning, programming language. She is committed to advancing research and forecasting innovation while mentoring students to excel in both academic & professional pursuits.

Ms. G. SATHWIKA is a postgraduate student pursuing a MCA in the Department of Computer Applications at QIS College of Engineering & Technology, Ongole an Autonomous college in Prakasam dist. She completed her undergraduate degree in BCA (Computers) from ANU. With a keen interest in research and practical learning, She is actively involved in academic projects and technical activities related to his field.