Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 23 Issue 3 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Mobile Adhoc Networks and Networking-An Overview of Existing Intrusion Prevention Techniques and Predictive Intrusion Prevention

By Michael Hosein & Jedidiah Aqui

University of the West Indies St. Augustine

Abstract- Intrusion Prevention in computer networking refers to the set of techniques and technologies used to detect and prevent unauthorized access, malicious activities, and attacks on a network. It involves actively monitoring network traffic, identifying potential threats or anomalies, and taking action to mitigate or block those threats. In the realms of Mobile Adhoc Networks and computer networking, substantial work has pointed to the gaps experienced with respect to proactively identifying and mitigating risks and network malicious behaviours and attacks. This paper seeks to highlight the existing intrusion detection and prevention techniques currently being utilized in MANETS and general computer networking and how the introduction of the novel Risk Profile approach based on Axiom theory can be utilized or integrated to improve the accuracy of existing models of Intrusion Detection and Prevention systems.

Index Terms: *IDS, IPS, manets, attacks, anomalous, risk, Malicious.*

GJCST-E Classification: *ACM Code: C.2.2*

Strictly as per the compliance and regulations of:

Mobile Adhoc Networks and Networking–An Overview of Existing Intrusion Prevention Techniques and Predictive Intrusion Prevention

Michael Hosein [α] & Jedidiah Aqui [σ]

Abstract- Intrusion Prevention in computer networking refers to the set of techniques and technologies used to detect and prevent unauthorized access, malicious activities, and attacks on a network. It involves actively monitoring network traffic, identifying potential threats or anomalies, and taking action to mitigate or block those threats. In the realms of Mobile Adhoc Networks and computer networking, substantial work has pointed to the gaps experienced with respect to proactively identifying and mitigating risks and network malicious behaviours and attacks. This paper seeks to highlight the existing intrusion detection and prevention techniques currently being utilized in MANETS and general computer networking and how the introduction of the novel Risk Profile approach based on Axiom theory can be utilized or integrated to improve the accuracy of existing models of Intrusion Detection and Prevention systems. With a dual purposed aim of bolstering public confidence in utilizing MANETs and improving the security posture of networks which depend heavily on Security controls to protect their information and assets.

Index Terms: IDS, IPS, manets, attacks, anomalous, risk, Malicious.

I. Introduction

Intrusion prevention, as mentioned previously, refers to the set of techniques and technologies used to detect and prevent unauthorized access, malicious activities, and attacks on a network. Furthermore, the primary goal of network intrusion prevention is to protect the network infrastructure, systems, and data from various types of attacks, such as denial- of- service (DoS) attacks, malware infections, unauthorized access attempts, and network exploits.

While the majority of intrusion detection and prevention systems and frameworks strive to achieve the aforementioned objectives, research highlights a persistent gap in IDPS—specifically, the challenge of accurately predicting and preventing potential future attacks without a notable increase in false positives. Addressing this, there is a crucial demand for the development of predictive intrusion prevention techniques that move beyond reliance solely on knowledge-based approaches derived from past attack types. Instead, there is a call for incorporating probability and risk- based criteria, empowering IDPS to proactively anticipate and thwart potential attacks before their occurrence.

In the investigations detailed in [1], [2] and [3] evidence of a lack of risk based approaches within MANETS were unearthed and a solution founded upon 'Axiom Theory' was developed to provide the probabilistic means required to establish the full picture of risk associated with a MANET and establish an accurate numerical value of Risk associated with the given MANET. In the upcoming papers [4] and [5], the developed solution was tested against current MANET and network traffic which stemmed from numerous real world networks such as:

- Public MANETS
- Military Network Traffic
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Mobile Networks
- VANETS

Whereby it was able to produce accurate representations of risk levels associated with the pertinent networks based on the Axiom criteria used in the Risk Profile formula.

The focus of this paper is to firstly establish the state of contemporary predictive Intrusion Detection and Prevention techniques via the review of literature and related works and secondly to integrate the 'Axiom Based' Risk Profile approach of the previous papers into Intrusion Detection and prevention systems and frameworks to address the aforementioned problem, enable or further bolster the accuracy of their prediction capabilities and establish another layer of controls in accurately addressing risk within Manets and computer Networking with the integration of both impact based and likelihood based data.

II. Literature Review

In this section, we look at the state of the current body of research surrounding MANET and Network predictive intrusion prevention techniques. An overview of the frameworks and systems currently in use will be conducted whereby a comparative analysis and introduction to MANET Risk Profile via axiom theory

Author α σ: Department of Computing and Information Technology University of the West Indies. St. Augustine, Trinidad and Tobago. e-mail: aqui2_jed@yahoo.com

would be discussed in the "Results and Discussion" and "Future Work" section.

In the work done by [6] a review of Network Intrusion Detection Systems (NIDS) was conducted whereby the commonly faced problem of false positives and the generation of a high volume of low-quality alerts was further dissected. This lead to the critical review of the state-of-the- art cyber- attack prediction solution which was based on NIDS Intrusion Alerts, its models and limitations. The solution utilized a technique known as 'intrusion alert correlation (AC) which included similarity-based, statistical- based, knowledge-based, and hybrid-based approaches.

The paper further elaborates that the technique deployed places reliance on raw networking alerts recieved and subsequently seeks to identify the association between different alerts and classifies or contextualize information into their pertinent categories all in an effort to predict a forthcoming alert/attack. The paper highlighted the current state of NIDS post-processing approaches to overcome the limitations of NIDS. The below diagram represents the taxonomy of existing alert correlation approaches which are classified as:

- *Statistical-based:* The basic idea of these approaches is that relevant attacks have similar statistical features, and a proper classification can be found by detecting these similarities.
- *Knowledge-based:* Based on two main components which are, scenario-based approaches to predict multi-step attacks and concequence-based which observe and control implications of alerts and existing knowledge in the network and then predict the security event.
- *Similarity-based:* Defined as the similarity between two alerts or alert clusters. This approach is known to cluster similar alerts in time to reduce the amount of alerts and increase its ability to discover known attacks.

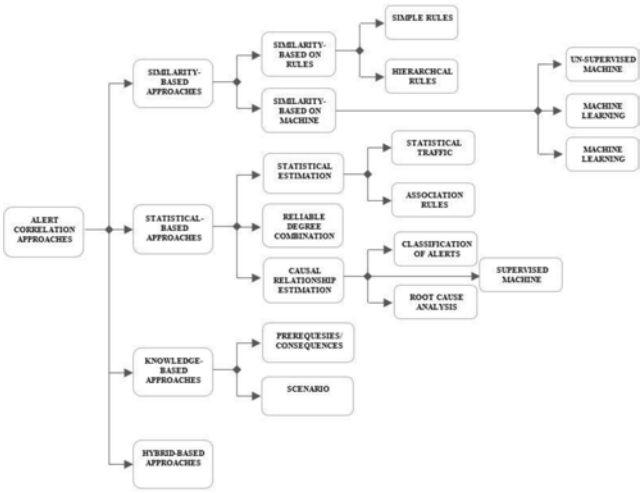

Fig. 1: Showing the taxonomy of Alert Correlation Approaches

As heavy reliance was placed on alerts and alert correlation, to address the limitations of the previously stated model, an alert correlation model was developed to ensure effective, efficient and accurate alerts were utilized for intrusion classification and prediction as shown in the below figure:

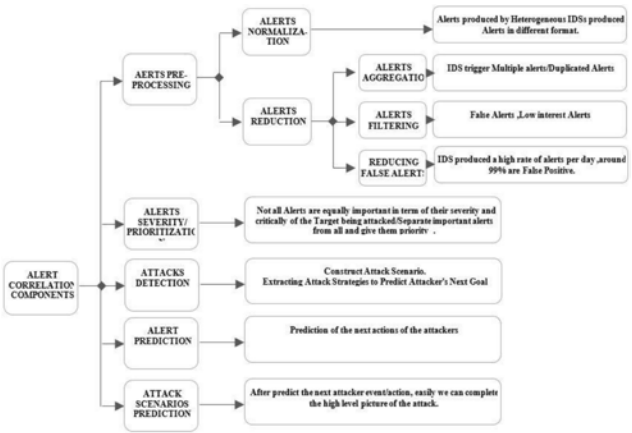

Fig. 2: Showing the Mapping of Alerts Correlation Components with Research Problems

In the work done by [7] another angle to intrusion detection and prevention from the traditional approach was taken. The proposed solution was aimed at cyber-attacks such as Stuxnet [8] and Maroochy [9] which target critical infrastructure to affect physical processes to cause harm. Rather than examine network packet behaviour or the possibility of anamolous behaviour or malicious attacks within the network, this approach utilized a payload analysis-based Intrusion prevention system. The embedded process prediction Intrusion Prevention System (EPPIPS) examined packets that were destined for a programmable Logic Controller (PLC) which interacted with a physical process. If the EPPIPS predicted that these packets or programs were indeed harmful it would potentially prevent or limit the harm.

The paper further postulates that the EPPIPS system acts as a middleman or proxy process within the PLC to act as the innermost layer of defense relative to the PLC in the case of any cyber-attacks. It addresses the immediate risk of a malicious payload that can interact with a Supervisory Control and Data Acquisition (SCADA) system and cause destruction, inefficiencies, and sabotage of cyber-physical systems. The work can be viewed as a variant of existing IDSs and IPSs as it focuses primarily on detecting malicious payloads that are sent to SCADA systems via the programmable Logic Controller. Emphasis is therefore placed on the calculation of possible effects that these malicious payloads can incur on the system and depending on the pertinent risk, possible preventative measures are enforced by the EPPIPS.

The studies done in [10] an examination of the numerous cyber attacks and their increasing frequencies was under- taken. It was noted that despite the existence of advanced cyber-defence systems, attacks and intrusions were still very prevalent. The studies highlighted the current or traditional operations of defence systems which attempt to:

- Block previously known attacks
- Stop ongoing attacks
- Detect occurred attacks

and their inability to minimize the damage caused by an attack which is catastophic. This pointed to the need for not only for improved intrusion detection systems but also intrusion prediction. The paper highlighted the need for more robust intrusion prediction systems by examining and investigating existing intrusion prediction systems as well as the current intrusion detection systems. The usage of improved prediction techniques was proposed with an aim of improving security capabilities for defence systems. The paper primarily sheds light on the gaps of existing intrusion defence systems as well as the necessary improvements required for intrusion prediction systems.

In [11] an ensembles approach towards intrusion detection and prediction was utilized to improve anomaly detection accuracy in a network intrusion environment. The paper indicates that the learning mechanism is based on automated machine learning and the prediction model is based on the Kalman filter. This approach was developed in light of the expeditious rise in the development of network and communication technologies. The paper highlighted that with an increase in pervasive computing networks such as the Internet of Things (IoT), an enormous amount of data is generated.

The data generated is considered to be high-dimensional as it consists of a variety of meta-data fields which pertain to the type of network the data was captured from. Additionally, IoT creates another challenge as diverse datasets which stem from various IoT devices makes it difficult for rule-based approaches for analysis of enormous data. The proposed IDS based on the ensemble of prediction and learning mechanisms is based on autoML. It is based on autoML to address the issue of nonlinear and high dimentional data. The paper highlighted that work had been done in both Convolutional neural networks (CNN) and long short-term memory (LSTM) in separate streams. Whereby, for data nonlinearity has been addressed in CNN and LSTM [12], [13], [14] and high dimensional data in CNN and LSTM are handled by a deep learning paradigm, [15], [16], [17].

The automated neural architecture search paradigm was shown as improving the accuracy of the learning model using parameter optimization and an optimal Kalman filter-based IDS is produced using, measuring and updating errors. It was found that the usage of the o-DNN and Kalman filters together created the ensemble intrusion detection model which was based on the weighted voting mechanism. The below is a conceptual diagram of the ensemble IDS:

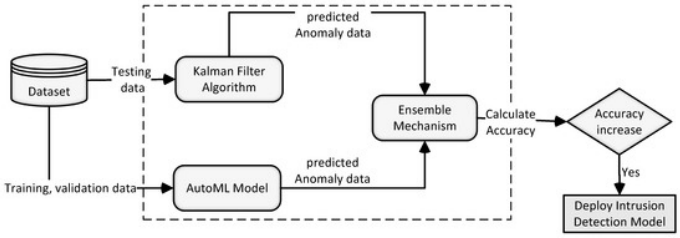

Fig. 3: Showing the Conceptual Diagram of Ensemble of Learning and Prediction Mechanism for Anomaly Detection

The paper [18] focuses on the development of an intrusion prevention system to overcome the static signature detecting mechanisms to identify intruders that exists in all host-based IPSs. This system was proposed within the context of quick evolution of IPS to provide high levels of security such as, which may replace existing security solutions, such as firewalls and anti-viruses. The solution encompasses a four-tier host based IPS that uses data mining technique known as "Decision Tree". This technique is utilized in the capacity of a detecting mechanism in the IPS. The IPS's decision tree consist of choices such as:

- Most infected computer resource by intruders
- Most targeted computer resource by intruders

As opposed to static signature databases. The paper sheds light on three experiments conducted with the proposed solution in an effort to assess the effectiveness of the IPS to classify untruders correctly.

In paper [19] the work explores the absence of widely accepted metrics for assessing information security issues and identifies the lack of empirical data validation as a contributing factor. The authors investigate the potential use of metrics derived from security devices, specifically intrusion detection and prevention system (IDPS) alert events, as indicators of security incidents. By analyzing IDPS data from a large organisation with 40,000 computers, the researchers conducted an empirical case study. The findings suggest that alert characteristics can effectively depict trends in certain security concerns, thereby serving as indicators of security performance. This information can aid security experts in prioritizing security inspections and developing new rules for incident prevention.

The paper did not focus directly on specific intrusion prevention systems but rather the indicators of key security events and incidents. The general approach encompassed analyzing 'big-data' which consisted of security alerts which were captured from 40,000 endpoint devices in the organisation. This paper focuses more on indicators of security performance versus the ability to pro-actively identify and remediate risk within the network.

The research [20] introduces a system called E-NIPS (Event-based Network Intrusion Prediction System) that goes beyond the capabilities of intrusion detection systems (IDSs) by not only detecting attacks but also predicting future potential attacks. The system is designed to partition network penetration scenarios into multiple phases based on the sequence of events during an attack. Each phase consists of attack classes that serve as precursors to attack classes in the subsequent phase. Attack classes represent sets of attacks with similar objectives, enabling generalization of network penetration scenarios and reducing the prediction engine's workload. The prediction of future attacks is based on the detection of attack classes in earlier phases of a penetration scenario.

The proposed automatic intrusion prediction system aims to provide critical time for network fortification, alert networkadministrators about possible attacks, and mitigate the dam- age caused by attacks. The paper describes the architecture, operation, and implementation of E-NIPS, and evaluates a prototype implementation using commonly occurring network penetration scenarios. The experimental results demonstrate that the prototype effectively provides valuable information about the occurrence of future attack events.

Finally, the work done by [21] can be viewed as the closest model towards the proposed predictive intrusion Detection and prevention approach/system of this thesis. The research takes a closer examination on cloud computing and the associated risks involved. The paper goes on to speak on the fact that cloud computing is the new paradigm which exploits already existing computing technologies in a new framework. Therefore alluding that cloud computing also inherited computing problems that are still challenging. The paper focuses on the challenge of cloud computing security as it requires strong security systems to protect the system and the valuable data stored and processed in it.

In addressing the security concerns of cloud computing, the topic of intrusion prevention was explored whereby it was found that typical IDPSs do posses limitations such as:

- Attacks being detected at the time that the damage of the attack was already done.
- Inability to deal with the speed and diversity of emerging cyber threats/attacks.

The proposed solution of this paper involves an Intrusion prediction system which is capable of sensing an attack before it happens in cloud or non-cloud environments. The primary workings of this system ensure 2 core activities:

- Assessing the host systems vulnerabilities
- Monitoring the network traffic for attack preparations.

These core activities are executed in the newly proposed method of statistical selective analysis for network traffic searching for an attack or intrusion indication which forms part of the first module. The second module of the system consists of vulnerability assessements which search for weak-nesses and faults in the identified system and subsequently measures the probability that the system can be compromised via a cyber-attack. And the third module also known as the prediction module performs the combination of outputs from the first and second modules, performs a risk assessment and subsequently gives a reading on the probability of an attack for that given network.

What should be noted with this system, is the method in which risk is calculated as well as the inputs required for a fair-accurate risk calculation. A comparative analysis would be done in the "Discussion" section which dissects the uniqueness of the proposed risk calculation of this paper and the risk profile calculation using axiom theory.

III. Methodology

The methodology deployed in this research of the existing body of studies in the field of:

- Intrusion Prevention systems and methodologies
- Intrusion Prediction systems and methodologies
- Predictive Intrusion Detection and Prevention systems and methodologies

Consist primarily of qualitative research and analysis geared towards further understanding and discussing the current uses and applications of IDS and IDPS systems. Emphasis was placed on the methods and systems that utilized probability or predictive based methods to ascertain risk levels within networks.

This methodology ensured that Risk Management and Risk Predictions and response plans were observed not only in the sphere of MANETS but in the general area of computer networking. The over-arching aim was to establish a position on contemporary IDS and IDPS systems which utilized similar approaches or techniques in ascertain risk levels and further compare this work to the developed "MANET Risk Profile determination via axiom theory" of the current thesis.

The work done can be seen as the foundation for introducing an integration of the "MANET Risk Profile" approach in the realm of general networking as well as an additional layer of control in identifying and proactively remediating potential network threats.

IV. Discussion

Based on the qualitative analysis conducted it was found that there was a plethora of different ways in which intrusion detection and intrusion prediction occurred. It was observed in one approach that primary reliance was placed on intrusion alerts with the aim of identifying associations among alerts, categorizing them accordingly and forming the basis for a more accurate Intrusion Prediction. In this model, this information was identified as an input into an Intrusion Detectionn System (IDS).

In another paper, it was observed that the role of intrusion detection and prevention was primarily focused on malicious attacks that target physical equipment and infrastructure. Instead of the usual approach of examining network traffic and trying to analyze packet behaviour or identify possibly malicious nodes, the paper focused on analyzing malicious payloads that were destined for the programmable Logic Controller in physical machines. The proposed intrusion prevention solution acted as a middleman or an additonal layer of control between transmitted payloads and the PLC of Supervisory control and Data Acquisition (SCADA) equipment.

Furthermore it was observed that other papers utilized a combination of techniques in addressing both the early detection and prevention of intrusions before they occur such as using an ensembles approach which utilized automated machine learning for the threat learning module and Kalman filtering for threat prediction. Another utilized a decision tree methodology whereby the technique was utilized in the capacity of a detecting mechanism in the IPS and some of the choices would have ranged from "most infected computer resource by intruders" to "most targeted computer resource by intruders".

Another noteable approach observed was the usage of event based network intrusion detection, which in design, was aimed at partitioning network penetration scenarios into multiple phases based on the sequence of events during an attack. A subsequent categorization of attacks into attack classes was done and utilized for generalizing network penetration scenarios and further inmproving the efficiency of the system's prediction module. In this approach reliance was placed on network penetration testing activities and results to further bolster the accuracy of attack predictions.

The work conducted can be noted as substantial, however there were some noteable re-occurring themes that were observed and stated below:

- Most of the observed intrusion prediction models were within the domain of general networking and not Mobile Adhoc Networks.
- Most of the identified approaches whilst different methods of executions were observed, they lacked the actual calculation of Risk and correlation to a numerical risk score.

One of the cornerstones of the Axiom Theory Risk Score calculation is the numerical representation of Risk which can subsequently be categorized accordingly and give an accurate picture of risks associated with a given MANET. Of all papers researched, [21] was identified as one of the closest models to the proposed method of risk calculation. Part of the methodology of proactively identifying and implementing controls to prevent attacks on the network was the usage of a risk scoring calculation. Risk was calculated via the below formula:

$$Risk = Ex\ P\ (Th_{\infty})$$

Whereby:

- Ex = The level of exposure
- Th_{∞} = The probability of an absolute threat

This method of Risk calculation assimilated both threat and likelihood factors into the calculation of risk, however when compared to the Axiom Theory Risk Calculation, some stark observations and differences were noted. [19]'s approach was aimed primarily at resolving cloud and to an extent non-cloud intrusions within the domain of a typical cloud or network architecture setup. This setup would comprise of network devices such as:

- Switches
- Routers
- Modems
- Firewalls

This method is not suitable for MANETS as MANETS are infrastructureless and do not consist of a typical network setup but rather interconnected and rapidly changing endpoint nodes.

Another observation was the overhead required to sustain the model would require large amounts of resources for processing of data and analyzing packet behaviour to feed into the prediction module. This type of calculation assumes that the environment would primarily be a cloud environment where resources are easily scalable per network requirements. This may not be suitable for an infrastructureless setup such as manets which have very limited resources and is dynamic.

Whilst the method of acquiring information to generate the risk score was very detailed, a point noted in the score's calculation was that the score would increase by 1 point for every scan performed on a network device. When observed this has the potential to skew the final Risk Score and subsequently skew the prediction results.

When observing the Axiom Theory Risk Profile formula, in its design and also its performance, it was observed that it was easily adaptable to MANETS as it was lighter weight in terms of the inputs required to generate the score as well as easily customizable as Axioms could be added or removed depending on the level of granularity required for the specific MANET.

It was also noted that the Axiom Theory Risk Profile formula had an additional advantage of acting as a second or third layer of defence in organisational networks, due to its level of flexibility and adaptability in terms of the classifying criteria for risk. This means that it can be easily integrated with Next Generation Firewalls (NGFWs) to further bolster the accuracy of intrusion prevention and enforce predictive intrusion prevention based on the Risk Apetite of a given organisation.

V. Conclusion

In summary, this paper's examination underscores the substantial body of work and research in the dynamic field of intrusion detection, prevention, and prediction. Notably, diverse methods have been devised and implemented in various contexts, some geared towards anticipating intrusions, while others focus on fortifying network infrastructure and physical systems reliant on network communications. Despite these advancements, significant gaps persist, particularly in the domain of ascertaining risk scores to enhance the efficacy of predictive intrusion detection and prevention systems. A notable observation is that the majority of predictive methods in this domain are applied in the broader context of general computer networking, lacking specificity tailored to the unique challenges presented by Mobile Ad-Hoc Networks (MANETs). The inherent infrastructureless nature of MANETs adds complexity to enforcing robust risk management compared to traditional network setups with diverse network devices, as discussed. Furthermore, one of the examined papers revealed a method employing a risk score approach in intrusion prediction and prevention. However, upon comparison with the Axiom-based Risk Score methodology, a discernible disparity emerged in its adaptability across various network types and the perceived level of accuracy when juxtaposed with the latter. These findings underscore the need for targeted approaches, specifically tailored to the distinct characteristics of MANETs, to advance the field of predictive intrusion detection and prevention.

VI. Future Work

The Forthcoming Endeavors in this Research Will Entail Seamlessly Integrating the Manet Axiom Theory this Incorporation Signifies an Augmented Layer of Control and Predictive Analysis within Contemporary Predictive Intrusion Detection, Serving as a Proactive Measure to thwart Suspected Attacks. The Primary Context for this Integration is within Corporate Network Settings, Where an Assortment of Intrusion Prevention Systems-Including Network Intrusion Prevention Systems (Nips), Wireless Intrusion Prevention Systems (Wips), and Host Intrusion Prevention Systems (Hips)-is Routinely Employed. This Model is Poised for Smooth Integration into Next-Generation Firewalls (Ngfws), Enhancing their Capacity to Predict and Identify Malicious Network Behavior With Heightened Accuracy and Efficiency. Consequently, it Fortifies the Enforcement of Rules Aimed at Preventing Unauthorized Entry into the Network.

References Références Referencias

1. M. Hosein and J. Aqui, "Mobile Adhoc Networks - An Overview of Risk Identification, Intrusion Detection and Machine Learning Techniques used," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICM-NWC), Tumkur, Karnataka, India, 2022, pp. 1-5, doi: 10.1109/ICMNWC56175.2022.10031757.

2. J. Aqui and M. Hosein, "Mobile Ad-hoc Networks Topic Modelling and Dataset Querying," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-6, doi: 10.1109/ICM-NWC56175.2022.10031921.
3. J. Aqui and M. Hosein, "Mobile Adhoc Networks - Establishing Initial Risk Profiles utilizing ML Techniques," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-5, doi: 10.1109/ICMNWC 56-175.2022.10031628.
4. J. Aqui and M. Hosein, "Mobile Adhoc Network Risk Profiles An overview of Existing Network Traffic Datasets to determine Ideal Axiom Criteria," unpublished.
5. J. Aqui and M. Hosein, "Mobile Adhoc Network Risk Profiles Establishing MANET and Network Risk Profiles," unpublished.
6. Albasheer, H.; Md Siraj, M.; Mubarakali, A.; Elsier Tayfour, O.; Salih, S.; Hamdan, M.; Khan, S.; Zainal, A.; Kamarudeen, S. Cyber- Attack Prediction Based on Network Intrusion Detection Systems for Alert Correlation Techniques: A Survey. Sensors 2022, 22, 1494. https://doi.org/10.3390/s22041494.
7. A. W. Werth and T. H. Morris, "Intrusion prevention for payloads against cyber-physical systems by predicting potential impacts," Journal of Cyber Security Technology, vol. 6, no. 3, pp. 113–148, 2022. doi:10.1080/23742917.2022.2088113
8. R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," IEEE Security and amp;amp; Privacy Magazine, vol. 9, no. 3, pp. 49–51, 2011. doi:10.1109/msp.2011.67
9. M. Abrams and J. Weiss, "Malicious control system cyber security attack case study: Maroochy Water Services, Australia," MITRE.
10. M. Abdlhamed, K. Kifayat, Q. Shi, and W. Hurst, Information Fusion for Cyber-Security Analytics. SPRINGER INTERNATIONAL PU, 2018.
11. Imran, F. Jamil, and D. Kim, "An ensemble of prediction and learning mechanism for improving accuracy of anomaly detection in network intrusion environments," Sustainability, vol. 13, no. 18, p. 10057, 2021. doi:10.3390/su131810057.
12. Y. Jiang, F. Yang, H. Zhu, D. Zhou, and X. Zeng, "Nonlinear CNN: Improving cnns with quadratic convolutions," Neural Computing and Applications, vol. 32, no. 12, pp. 8507–8516, 2019. doi:10.1007/s00521019-04316-4
13. J. Gonzalez and W. Yu, "Non-linear system modeling using LSTM Neural Networks," IFAC-PapersOnLine, vol. 51, no. 13, pp. 485–489, 2018. doi:10.1016/j.ifacol.2018.07.326.
14. Y. Tan et al., "LSTM-based anomaly detection for non-linear dynamical system," IEEE Access, vol. 8, pp. 103301–103308, 2020. doi:10.1109/access.2020.2999065.
15. P. Shamsolmoali, D. Kumar Jain, M. Zareapoor, J. Yang, and M. Afshar Alam, "High-dimensional multimedia classification using deep CNN and extended residual units," Multimedia Tools and Applications, vol. 78, no. 17, pp. 23867–23882, 2018. doi:10.1007/s11042-018-6146-7.
16. O. Cheikhrouhou et al., "One-dimensional CNN approach for ECG arrhythmia analysis in fog-cloud environments," IEEE Access, vol. 9, pp. 103513–103523, 2021. doi:10.1109/access.2021.3097751.
17. K. Praanna, S. Sruthi, K. Kalyani, A. S.Tejaswi, "A CNN-LSTM Model for Intrusion Detection System from High Dimensional Data," J. Inf. Comput. Sci. 2020, 10, 1362–1370.
18. A. Al-hamami and T. Alawneh, "Developing a host intrusion prevention system by using Data Mining," 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT), 2012. doi:10.1109/acsat.2012.103.
19. R. S. Miani, B. B. Zarpelao, B. Sobesto, and M. Cukier, "A practical experience on evaluating intrusion prevention system event data as indicators of security issues," 2015 IEEE 34th Symposium on Reliable Distributed Systems (SRDS), 2015. doi:10.1109/srds.2015.17.
20. P. Kannadiga, M. Zulkernine, and A. Haque, "E-NIPS: An event based network intrusion prediction system," Lecture Notes in Computer Science, pp. 37–52. doi:10.1007/978-3-540-75496-1.3.
21. "Intrusion prediction system for cloud computing and network based systems," Guide books, https://dl.acm.org/doi/book/10.5555/AAI28329182 (accessed Jul. 13, 2023).