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 – Integrating Risk Profiles into Intrusion Prevention Systems to Improve Predictive Intrusion Prevention

By Aqui Jedidiah & Hosein Michael

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 general computer networking, substantial work has pointed to the gaps experienced with respect to proactively identifying and mitigating risks and network malicious behaviours and attacks. Further research was conducted to establish the current state of contemporary intrusion detection, prediction and prevention techniques and their effectiveness to pro-actively identify and mitigate network attacks and malicious activity. However, it was found that the techniques utilized were very few or required futher accuracy improvements and for the identified effective techniques, they required substantial amount of data processing power and a robust network architecture to support its implementation.

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

GJCST-E Classification: *ACM Code: C.2.0*

Strictly as per the compliance and regulations of:

Mobile Adhoc Networks and Networking – Integrating Risk Profiles into Intrusion Prevention Systems to Improve Predictive Intrusion Prevention

Aqui Jedidiah [α] & Hosein Michael [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 general computer networking, substantial work has pointed to the gaps experienced with respect to proactively identifying and mitigating risks and network malicious behaviours and attacks. Further research was conducted to establish the current state of contemporary intrusion detection, prediction and prevention techniques and their effectiveness to pro-actively identify and mitigate network attacks and malicious activity. However, it was found that the techniques utilized were very few or required futher accuracy improvements and for the identified effective techniques, they required substantial amount of data processing power and a robust network architecture to support its implementation. The work of this paper, introduces the integration of the MANET Risk Scoring methodology based on Axiom theory into the realm of general networking. All in an effort to increase the efficiency and accuracy of existing predictive intrusion prevention systems such as next generation Firewalls in corporate networks.

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

I. Introduction

Intrusion Prevention as mentioned previously in the abstract, involves the set of techniques and technologies used to detect and prevent unauthorized access, malicious activities, and attacks on a network. The common or normal uses of typical intrusion detection and prevention systems saw the usage of techniques to detect attacks and prevent their effects after occurrence within a given network. This however was viewed as a short-comming of these models of intrusion detection and prevention systems as their response times were inadequate and often occurred after damage was already done to the existing network infrastructure.

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

According to papers [1] and [2] the general reactive approach to intrusion detection and prevention was due to a lack of risk-based studies and the prevalence of impact-based studies in the realm of mobile adhoc networks (MANETS). This view was seen as as siloed and thus to address this gap, a solution founded upon 'Axiom Theory' was developed in [3]. This theory proved vital for solving the issues of probability-based approaches in addressing risk within manets and creating a new model for predictive intrusion prediction and prevention for MANETS.

After the probabilistic method of risk score generation for MANETS was established in [3], it was then tested on several real-world network traffic and Manet datasets as per the work of [4] and [5] which would have stemmed from various sources such as, *Public MANETS, Military Network Traffic, Intrusion Detection Systems, Intrusion Prevention Systems, Mobile Networks, VANETS*. The results produced a Risk Profile or Risk Score(a numerical representation of risk) followed by a classification criteria for the given MANET in question and also established a new and accurate lightweight method for risk calculation for infrastructure-less networking setups such as MANETS.

The prospects of having an easily scalable method of calculating risks within MANETS also posed a new method or in some cases another layer of control within general network studies surrounding predictive intrusion detection and prevention. The work of [6] saw an overview of existing predictive network intrusion detection and prevention systems and techniques. It was found that whilst there were various ways in which systems predicted netwoork intrusions or malicious behaviour there was little to no systems in place to accurately predict and prevent an attack before it occurred on the network with the exception of one [7] which undertook a similar methodology but was seen as not easily adoptable or scalable for different networking contexts.

The work of this paper focuses on proposing a method to integrate the axiom-theory risk score calculation methodology into the field of general networking which speaks to typical network setups

which consists of many tools and devices both hardware and software that make up the network. It also disects the key diffrerences in approaches deployed in [7] and the proposed system to address the issue of scalability, practicality and applicability to a plethora of varying networks.

II. Literature Review

In this section, a summary of the previous research conducted in [6] is stated as this paper's work can be viewed as the proposition of the solution to address the gaps identified in the previous paper.

In the work done by [8] 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.

In the work done by [9] another angle to intrusion detection and prevention from the traditional approach was taken. The proposed solution was aimed at cyber-attacks such as Stuxnet [10] and Maroochy [11] which target critical infrastructure to affect physical processes to cause harm. Rather than examine network packet behaviour or the possibility of anamolous be- haviour or malicious attacks within the network, this approach utilized a payload analysis-based Intrusion prevention sys- tem. 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 studies done in [12] an examination of the numerous cyberattacks 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.

In [13] 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 spoke to the increase in pervasive computing networks such as the Internet of Things (IoT), which generated an enormous amount of data which is considered high-dimensional as it consisted of a variety of meta-data fields. This created a challenge for rule-based approaches to analyse the 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 [14], [15], [16] and high dimensional data in CNN and LSTM are handled by a deep learning paradigm, [17], [18], [19].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 paper [20] focused 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 [21] the work explored 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 investigated 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

suggested that alert characteristics can effectively depict trends in certain security concerns, thereby serving as indicators of security performance. This paper focuses more on indicators of security performance versus the ability to pro-actively identify and remediate risk within the network.

The research [22] introduced a system called E-NIPS (Event-based Network Intrusion Prediction System) that went beyond the capabilities of intrusion detection systems (IDSs) by not only detecting attacks but also predicting future potential attacks. The system was designed to partition network penetration scenarios into multiple phases based on the sequence of events during an attack. Each phase consisted of attack classes that served as precursors to attack classes in the subsequent phase. Attack classes represented sets of attacks with similar objectives, enabling generalization of network penetration scenarios and reducing the prediction engine's workload. The prediction of future attacks was based on the detection of attack classes in earlier phases of a penetration scenario. The proposed automatic intrusion prediction system aimed to provide critical time for network fortification, alert network administrators about possible attacks, and mitigate the damage caused by attacks.

III. Methodology

The methodology of the proposed solution is envisioned within the context of an enterprise network. Two main approaches would be considered.

Approach 1: whereby the Axiom Theory predictive intrusion prevention system is placed before the enterprise's edge firewall as the first line of defence.

Approach 2: whereby the Axiom Theory predictive intrusion prevention system is placed after the enterprise's edge firewall as the second line of defence.

The primary technique of intrusion prevention utilized within this context is known as.

- *Policy Based - Intrusion Prevention*- This method employs security policies defined by the enterprise and blocks activity that violates those policies. This requires an administrator to set up and configure security policies.

There would also be to a lesser extent some elements of 2 other types of intrusion prevention techniques known as.

- *Signature Based - Intrusion Prevention* - This method matches the activity to signatures of well-known threats. However, one of the main drawbacks to this method is that it can only stop previously identified attacks and won't be able to recognize new ones.
- *Anomaly-based - Intrusion Prevention* - This method monitors for abnormal behavior by comparing random samples of network activity against a baseline standard. It is more robust than signature-based monitoring, but it can sometimes produce false positives.

However, the principle reason for utilizing a policy-based technique is due to the fact that the Axiom-Based approach for risk categorization acts as the first layer of defence before reaching the enterprise's firewall according to Approach 1. The following figure 1 is an example of an enterprise network layout.

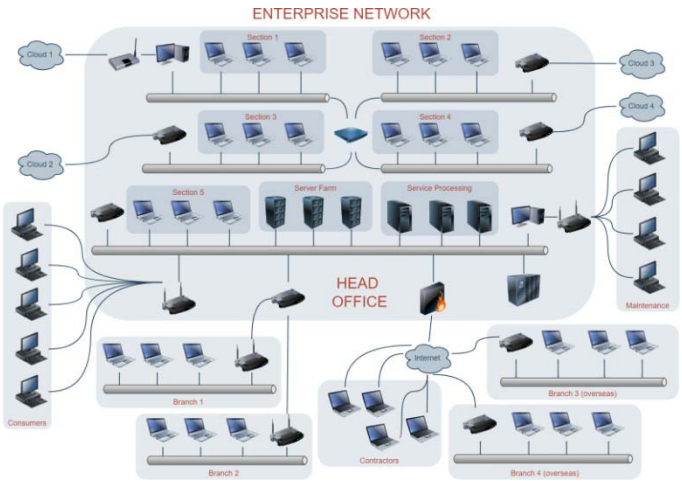

Fig. 1: Showing an Enterprise Network Setup

Approach 1

With the implementation of Approach 1, the enterprise network would now contain a change to the topology specifically between the internet and the firewall as shown in the below figure 2:

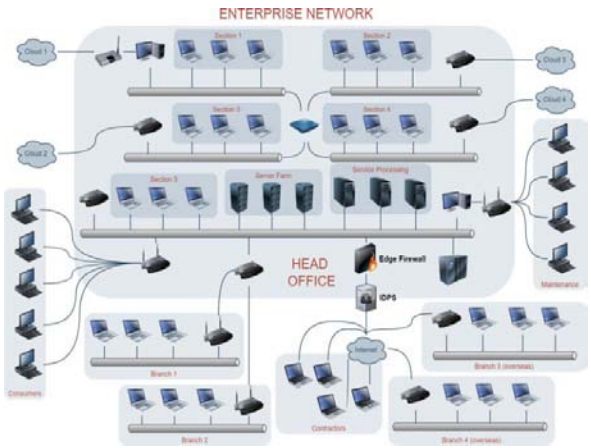

Fig. 2: Showing an Enterprise Network Setup - Approach 1

This change is necessary as the IDPS would act as the first line of defence and begin filtering and categorizing network packets entering the Head Office of the enterprise. This therefore allows the firewall to undertake a policy-based approach to incoming network traffic as it can now add additional rule categories to allow/prevent network traffic with a risk score of a particular value.

In this approach the IDPS would generate risk scores for incoming traffic and this in turn would be filtered to the firewall for processing and decision making for entry into the network. This alludes that the IDPS acts as the first-line of defence in the capacity of classifying incoming network traffic based on the defined Axioms, with the most generic axioms identifying malicious and anomalous packet behaviours and/or device types which are trying to send traffic to the internal network.

In approach 1's application of the axiom-based IDPS, the predictive capabilities are coined with the functions of the edge firewall to prevent attacks or malicious activity from causing harm to the network pro-actively. This also forms the basis of next generation firewalls which integrate with Intrusion detection and prevention systems.

Approach 2

With the implementation of Approach 2, the enterprise network would now contain a change to the topology specifically between the edge firewall and the Enterprise network as shown in the below figure 3:

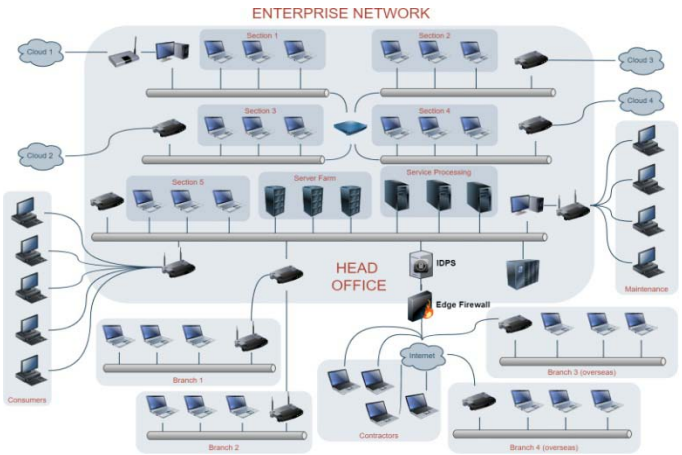

Fig. 3: Showing an Enterprise Network Setup - Approach 3

In this approach the IDPS acts as the second line of defence within the network and takes on the role of classifying risk and remediating accordingly as per risk apetite. Being the second line of defence means that there is a lesser chance of encountering network traffic that qualifies for any of the prescribed axioms. However, as the firewall aligns primarily with the Policy-based method of intrusion detection, this scenario allows for the IDPS to leverage both the Signature based and Anomaly Based methods of intrusion prevention more.

By leveraging both of these methods, it allows for the second line of defence within the network to continue performing background checks and/or

forensics whilst the firewall un- dertakes the majority of overhead in filtering and preventing malicious network traffic from entering. The combination of both the firewall and IDPS within this capacity also makes for a substantially stronger Network Architecture as the components work in parallel similar to next-generation firewalls.

IV. Discussion

In the "Methodology" section, it was observed that two (2) main approaches were proposed for the usage of the Axiom Theory predictive intrusion detection and prevention within the context of an Enterprise Network. They consisted of:

Approach 1: The Intrusion Detection and Prevention System was placed before the edge firewall, situated between the internet and the firewall as the first line of defence within the network.

Approach 2: The Intrusion Detection and Prevention System was placed after the firewall, situated between the edge firewall and the enterprise network as the second line of defence within the network.

Before delving further into both approaches however, the observations noted from the system implemented in [7] must be discussed. The paper [7] was noted as having a similar approach by way of establishing a risk score and categorizing Risk based on criteria of a heat map. Whilst the work was substantial, some stark differences and/or gaps were noted with respect to this approach and the proposed axiom solution:

- The solution was developed primarily for predicting and mitigating cloud security events and to an extent non- cloud security events.
- The solution was not easily deployable for varying Network Architectures such as VANETS, MANETS or peer to peer network as it required substantial meta-data to calculate the risk score.
- The solution requires considerable compute power for big data processing as it consists of 2 main modules for assessing the host's vulnerabilities and monitoring attack preparations within the network
- 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.

The Axiom-Based Risk Profile approach answers the concerns and shortcommings of the aforementioned gaps not only within the situation of Mobile Ad-Hoc networks and Vehicular Ad-Hoc networks but by merit of the previously stated approaches 1 and 2 it is easily integrateable with differing Network Architectures. This is possible because of the light- weight but accurate nature of the solution, the original design was primarily catering to the security needs of infrastructure- less networks such as MANETS. The aforementioned approaches 1 and 2 were examples of its integration within an Enterprise Network setting to further enhance the proactive security risk mitigation capabilities.

When observing Approach 1, it is noted that the role the proposed predictive IDPS (PIDPS) is more on the basis of classifying malicious/anomalous network behaviour, nodes and activities to inform the edge firewall. The predictive capability and pro-active prevention of network attacks is enforced by the egde firewall based on the Axiom criteria that it is allowed and prevented in its policy-based rule-sets which dictate the decision making process. In this approach the core function of the IDPS is predictive detection and informing for subsequent action-taking.

However, Approach 1 can also be used in another dynamic whereby the overhead is utilized by the IDPS to not only observe and classify network events and behaviours but also to execute the pertinent actions required based on the network traffic risk-levels. By enforcing this strategy, much overhead is reduced on the firewall as the heavy processing occurs at the IDPS level firstly. Axiom theory, allows for the scalability of processing of the risk classification approach by adding to the pool of axioms for classifying data. In other words the IDPS can both proactively detect and prevent malicious and anomalous network activity without the intervention of the firewall.

When observing Approach 2, it is noted that the role of the PIDPS centers on the basis of the traffic entering the network after passing through the edge-firewall. The majority of traffic processing is handled by the edge-firewall. This means that risk classification would occur at the second layer of defence as opposed to the first, by this occurring, the PIDPS acts as a secondary control before traffic enters and leaves the network. This means that greater levels of forensics and data processing can occur in the background as most of the processing of incoming traffic is handled by the firewall. It also means that machine learning techniques for network data processing is much more feasible with this approach as the PIDPS can be utilized to further bolster the resilience of the Network's Security posture and also form the basis for more accurate firewall ruleset updates based on new/emerging threats.

Approach 2 also allows for the classification of risk per-taining to network traffic leaving the Enterprise network. This therefore means that in the event a malicious user was able to infaltrate the Enterprise's network, the PIDPS is likely to identify this behaviour, classify and prevent from leaving the network and/or traversing the Network's Architecture to infect or affect other Network devices and services.

V. Conclusion

In conclusion, the research underscores the substantial benefits of incorporating the MANET Axiom Theory Risk Calculation methodology into the domain of Enterprise Networking. The comparative analysis revealed that both proposed approaches (1 and 2) of the Predictive Intrusion Detection and Prevention System (PIDPS) introduce an additional layer of control within the Enterprise's Network. Furthermore, they effectively address the limitations identified in a cloud-based approach that employs a similar technique-deriving a risk score, categorizing risk, and leveraging this information to predict and prevent intrusions in a network. A standout feature of the Axiom-Theory approach is its notable adaptability and scalability. This characteristic allows its application to transcend the constraints of infrastructure-less networking, extending its utility to general networking topologies that comprise numerous network devices and software. This versatility implies that enhancing the predictive detection and prevention of network threats can be achieved with heightened accuracy and scalability, tailoring the methodology to meet the specific requirements of diverse networks.

VI. Future Work

The future trajectory of this research will involve the implementation of the proposed approaches to seamlessly integrate Axiom-Based Risk Calculation into a standard network architecture. This signifies a crucial advancement, serving as the next phase in augmenting the capabilities of "next-generation firewalls" to anticipate and thwart network intrusions. Beyond fortifying firewall capabilities, this endeavor is positioned as an essential system/methodology designed to rectify the deficiency of accurate risk-based data, which is pivotal for synergizing with impact-based data in the realm of Network Security.

The overarching objective is to develop a functional model or prototype for implementation within an Enterprise Network. Subsequent to this development, rigorous testing will ensue to assess the accuracy of the generated results. This testing phase is integral in evaluating and quantifying the effectiveness of seamlessly integrating the innovative risk-based approach into the broader landscape of general networking.

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 Net-works and Wireless Communications (ICMNWC), Tumkur, Karnataka,India,2022,pp.1-5,doi:10.1109/ICMNWC56175.2022.10031757.
2. J. Aquiand M. Hosein,"Mobile Ad-hoc Networks Topic Modelling and Data set Querying, "2022IEEE 2nd International Con-ference on Mobile Networks and Wireless Communications (ICM-NWC), Tumkur, Karnataka, India, 2022, pp. 1-6, doi: 10.1109/ICM-NWC56175.2022.10031921.
3. J. Aqui and M. Hosein, "Mobile Adhoc Networks - Establishing InitialRisk Profiles utilizing ML Techniques," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICM-NWC), Tumkur, Karnataka, India, 2022, pp. 1-5, doi: 10.1109/ICM-NWC56175.2022.10031628.
4. J. Aquiand M. Hosein, "Mobile Adhoc Network Risk Profiles- An overview of Existing Network Traffic Datasets to determine Ideal Axiom Criteria, "unpublished.
5. J. Aquiand M. Hosein, "Mobile Adhoc Network Risk Profiles-Establishing MANET and Network Risk Profiles, "unpublished.
6. M. Hoseinand J. Aqui, "Mobile Adhoc Networks and Networking – An overview of Existing Intrusion Prevention techniques and predictive intrusion prevention, "unpublished.
7. "Intrusion prediction system for cloud computing and network based systems, "Guidebooks, https://dl.acm.org/doi/book/10.5555/AAI28329182. (access-ed Jul.13,2023).
8. 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.
9. A. W. Werth and T. H. Morris, "Intrusion prevention for pay loads 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.
10. R. Langner, "Stuxnet: Dissecting a cyber warfare weapon," IEEE Security and amp; amp; Privacy Magazine, vol. 9, no. 3, pp. 49–51, 2011. doi:10.1109/msp.2011.67
11. M. Abrams and J. Weiss, "Malicious control system cyber security attack case study: Maroochy Water Services, Australia, "MITRE.
12. M. Abdlhamed, K. Kifayat, Q. Shi, and W. Hurst, Information Fusion for Cyber-Security Analytics. SPRINGER INTERNATIONAL PU, 2018.
13. 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.

14. 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/s00521-019-04316-4.
15. J. Gonzalez and W. Yu, "Non-linear system modeling using LSTM Neural Networks," IFAC-Papers OnLine, vol. 51, no. 13, pp. 485–489, 2018. doi:10.1016/j.ifacol.2018.07.326.
16. Y. Tanetal.,"LSTM-based anomaly detection for non-lineardy-namical system, "IEEE Access, vol. 8, pp. 103301–103308, 2020. doi: 10.1109/access.2020.2999065.
17. P. Sham solmoali, D. Kumar Jain, M. Zareapoor, J. Yang, and M. Afshar Alam, "High-dimensional multimedia classification using deep CNNand extended residual units," Multimedia Tools and Applications, vol.78,no.17, pp.23867–23882, 2018. doi:10.1007/s11042-018-6146-7.
18. O. Cheikhrouhou et al., "One-dimensional CNN approach for ECGarrhythmia analysis in fog-cloud environments," IEEE Access, vol. 9, pp.103513–103523, 2021.doi:10.1109/access.2021.3097751.
19. 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
20. 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.
21. R. S. Miani, B. B. Zarpelao, B. Sobesto, and M. Cukier, "A practical experience one valuating 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.
22. P. Kannadiga, M. Zulkernine, and A. Haque, "E-NIPS: Anevent-based network intrusion prediction system,"Lecture Notes in Computer Science, pp.37–52. doi: 10.1007/978-3-540-75496-1.3.
23. 'Intrusion prediction system for cloud computing and network based systems, "Guide books, https://dl.acm.org/doi/book/10.5555/AAI28-329182 (accessed Jul.13).