JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

THE DEEP INTRU-NET FOR ANOMALY DETECTION IN MASSIVE IOT NETWORKS

[1]M.Lavanya, [2]J.Jayaprakash, [3]D.Chiranjeevi, [4]B.Thejaswini , [5]G.Tejasree

[1]Assistant Professor, [2,3,4,5]Student,
[1]Computer Science and Engineering,
[1]Mother Theresa Institute of Engineering and Technology, Palamaner, India

Abstract: The massive development of the internet of things enabled various applications in smart devices, mobiles, laptops, and equipment that are configured with the common internet to provide flexible access. numerous users benefited by the reliability of the internet as a common medium. on the similar scope of work, the intrusion attacks threaten the system security. The data stored in the cloud needs to be protected from network anomalies. The presented system is focused on development of novel deep learning architecture with tuned layers for better performance. The presented system considers the CICIDS2017 dataset. The system considers the CICIDS dataset as the reference information and creates an architecture using Deep Intru-Net to test. The dataset is divided into training data of 80% and testing data of 20%. The dataset holds the recorded patterns of network anomalies. The Deep Intru-Net learns the frequent pattern of anomaly in the network and detects the occurrence of similar patterns. The improved iterations increase the learning strength of the system. The performance evaluation is made using accuracy value estimation and the proposed network achieved 98% accuracy.

Index Terms - Intrusion detection, Deep learning, Network security, Anomaly detection, Machine learning.

I. INTRODUCTION

In the current development of 5G networks, the protection of data stored in the network is highly important. Securing the network from malicious activity is highly demanded to secure the huge data in the cloud. Network hazards occuring in the massive network impact the system security with loop holes or wormholes in the system. The research effort developed an intrusion detection system that automatically identifies malware or other random activities by decoding packets and checking them each time they join the network. In this research, we provide an IDSS equipped with a sound-emitting alarm system that may be activated in response to any potentially malicious event. [1]. Various network anomalies happen to be occurring in the system that extracts the large scale of confidential data, information on transaction data, system activity logs, follow up details are hacked by the third party. These activities need to be monitored by the system intrusion detection models. Because of the flexible usage of cloud protocol, people are accessing the cloud for various reasons. The more frequent access to the cloud also found it important to track the activity of the user. The malicious user can get access in between the activity of similar logons made frequently[2]. The intrusion attacks can be protected through

installing antivirus softwares, windows defenders, security guards etc. As a result, it is now easier for end users to upload data on a more frequent basis. Enable the port open to accept all inputs for a predetermined amount of time each time the user logs in to a particular network. Hackers and third-party users can exploit this key gap to gain access to the network grid's most sensitive data. Interruption recognition frameworks are little devices or programming that goes about as an entrance watch in the organization focuses to disregard the different action

during weighty traffic. Performed a study effort on a revolutionary triple intrusion detection system, in which the IDPS assures secure connection with SDN-IOT in terms of failure analysis, accuracy, precision, latency, traffic crown sensing, and other such things; they have employed fuzzy based authentication scheme. They came to the conclusion that more enhancements were required with models that preserved privacy and used new strong authentication [3].

The IDSS or so called intrusion detection system offers enhanced protection to the computers to protect the system data from various third party attacks. grid level security is provided by the firewalls. the basic protection strategy followed by the system through antivirus installations, troubleshooting the threats, malware protection tools are employed in common. various classifications of intrusion detection systems are discussed. The common categories of intrusion detection systems are described below.

NIDS: Network Intrusion detection system

NIDS are models preprogrammed to be initiated for a node based anomaly detection framework. The system tracks all the incoming patterns of data and formulates the presence of anomaly patterns. Firewall protection is implemented in common where numerous anonymous software entries are mapped.

System level Intrusion Detection

The system level intrusion detection system are networks connected with the IoT devices. The IDS system runs independently in the network activity and alerts the administrator on entry of intrusion attacks. the system control takes over the attack scenario if the alert is acknowledged. In case of resilient attack entry, the system control is vanished by the slow attacks and a part of the anomaly code is dumped into the system hidden location. From the hidden location, the malwares takes control of the system. Each system independently has an intrusion detection framework.

Protocol enabled Intrusions

The systems and devices connected over the massive Internet of things (IoT) network have various agents connected over the server. the attacks enter over the communication protocols and happen to be attacked. The simple HTTP link from the malicious user can take over the control of the system. The regular screening of HTTP links are implemented by the system to prevent network attacks.

Intrusion detection through Application

Application specific modules are impacted by the network attacks. a specific application is affected by the malicious activity. The application is getting updated from the internet. During the updation of software applications, the malicious pattern also gets updated. This kind of application based system is keenly monitored.

Hybrid Network

In certain cases the combination of above explained network intrusion, host based intrusion, application based intrusion are employed as Hybrid network.

Signature based IDSS (Start type from here)

Signature based detection model is used to screen the external anomalies through affixed pattern called signature verification. artificial neural network algorithm to match the pattern between the miscellaneous activity and given input data. In case of pattern recognition required for intrusion detection system the trained model is helpful to make the alignment. The signature based authentication is helpful to keep the secure environment in cloud per message. The concept of top for signature based intersection detection system is similar to that of Malware detection in IoT networks and mobile devices.

Anomaly based in two deduction systems or helpful to detect the malware Attacks coming over the network routers. The continuous tracking scenario is utilized to make the suspicious attack pattern detection within the connected Network and protrude mission learning models or analysed to prove the actual origin of the problem.

- The study focuses on gathering a variety of evidence from the literature regarding the demand for intrusion detection systems, evaluating the drawbacks of existing models, coming up with a concept that would allow us to proceed with the research on implementations of intrusion detection systems, and developing a novel methodology that improvises from the existing system.
- Deep Intru-Net with Resistant Propagation is the framework used to create the proposed model for deep learning. The future upgrade and understandings on arrangements would be talked about as well.

The rest of the paper is constructed with detailed literature background in section II. Followed with system tool selection, design perspectives in section III is discussed. Sections IV describe the design methodology adopted and followed by detailed results and discussions are given. The journal is concluded with future enhancement.

II. ABBREVIATIONS & ACRONYMS

- **NIDS -** Network Intrusion detection system
- **IDS** – Intrusion detection system
- **IDPS** - Intrusion detection protection system
- **IOT** – Internet of things
- **HTTP** – Hypertext transfer protocol

III. BACKGROUND STUDY

(Akhil Krishna et al., 2020) Research work has been carried out on an intrusion detection and prevention system using deep learning algorithms.

For both testing and training purposes, they employed the kddcup99 dataset. The implementation may be broken down into two categories: the first is for the detection of intrusion systems, and the [2] second is for the prevention of intrusion systems. The batch processing method known as MLP (Multi-Layered perceptron) is used in the suggested article, which achieves 91.4% accuracy in prediction.

(Zhigang Huang et al., (2019)) It came to the conclusion that advanced protocols allow improved security on IOT networks after doing research on outdoor and indoor resilience using a mutual authentication system. Their research included assaults such as relay attacks, MITM attacks, quantity attacks, and more.

(rafalKozik et al., 2014) the author published a research article that recommended employing Bayesian networks as a machine learning technique for the identification of cyber assaults. The query-based attack detection mechanism was the primary focus of the system. In the last section of the study, the authors state that the efficiency of the signature-based technique has to be increased, and that strong authentication IDSS are essential.

(M-Islaabudeen et al., 2020) In the context of MANER-Security, an assessment is made of the research work done on mobile ad-hoc network-based smart IDSS. They classified the data packets using an artificial neural network (ANN). ANN stands for artificial neural network. They said that categorization is a significant factor in the intrusion detection process. The development of a boat classifier may be seen here. It has been determined that the system is effective against uncommon assaults, DOS, and probing difficulties.

(Yue Jin, ZTian, et al., 2018) They conducted research on a WiFi-enabled IoT home intrusion detection system. They integrated a detection algorithm into an identifying router based on received signal strength indicator (RSSI) and made it possible to see the status of the whole home's security system through the Internet of Things. Using RSSI to secure the Internet of Things yielded satisfactory findings for the researchers, leading them to the conclusion that the suggested design maximises the fidelity of detection.

(F.Lin et al., 2018) In the proposed research and implementation of IDSS in edge-routed networks, the single-layered Min-max fair allocation method (SDMMF) is used to blend together analysis of DDoS attacks, detection of intrusions into edge networks, cloud security for edge nodes, and so on. In the last section of the article, they claim to have provided a practical answer to the issue of allocating resources across many hierarchies.

(Deval Bhamare et al., 2016)Their research focuses on the inequities and difficulties of supervised ML algorithms and real-time user interfaces. Network function virtualization (NFV) is a brand new way of working that was developed. Given that machine learning necessitates additional cloud security protocol for the ever-evolving cloud setting.

The purpose of the research was to get a better understanding of the difficulties associated with intrusion detection systems, such as those related to network performance, privacy, and energy usage. The article also covered topics including the difficulties of implementing IDS systems, research overlaps and impediments, and the restrictions of deep information collection. Various literature papers on intrusion detection system are comprehently studies here for learning existing challenges [11][12].

.IV. SYSTEM DESIGN

The CICID2017 dataset is a cyber-security-related dataset that was developed for the purpose of making the research of intrusion detection in computer networks easier to conduct. TCP, UDP, and HTTP are some of the network-level and transport-level protocols whose logs are included in this collection. Moreover, the dataset comprises logs of both benign and malicious network traffic. The information was gathered from a variety of resources, some of which included academic institutions, research facilities, and commercial businesses.

Researchers working in the area of network security make extensive use of the dataset in order to analyse and compare the effectiveness of various intrusion detection systems. It is now widely recognised as the gold standard for intrusion detection, and several research publications have made use of it to assess the effectiveness of the solutions they have provided. The CICID2017 dataset is an updated version of the earlier CICIDS datasets. It includes network traffic logs that are more diversified and up to date, making it a significant resource for academics and practitioners working on network security.

V. METHODOLOGY

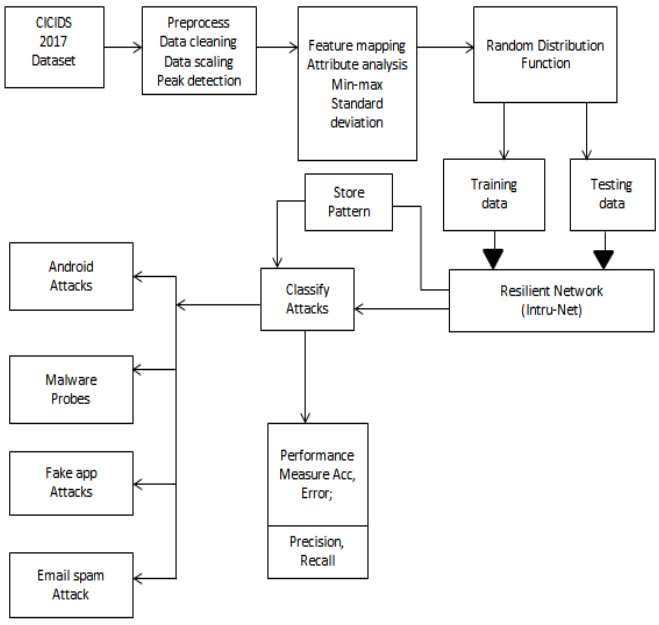

Fig 1. System architecture of Proposed Deep IntruNet

The block diagram illustrates the primary elements of an intrusion detection system as well as the information flow that occurs between those components. The first step in the procedure is the gathering of data on network traffic, which is followed by the pre-processing of the data to eliminate any superfluous or unnecessary information.
Then, the data is delivered to the component responsible for feature extraction. Here,unique features are extracted from the data representing network traffic in order to represent the data in a manner that is both more compact and more intelligible.
When the features have been extracted, they are sent on to the feature selection component, which is responsible for choosing the characteristics that are most important to the intrusion detection job based on the importance and relevance of those features.
After that, the chosen characteristics are sent on to the classification component, which makes use of a machine learning algorithm to determine if the data gathered from the network traffic is innocent or malicious.
In the last step, the performance of the classified data is assessed by the performance assessment component. Based on the findings, a decision is made about whether or not to allow the network traffic to get through or to block it.

Fake app

A malicious software programme that is created with the intention of fooling users into thinking that it is a real app is referred to as a fake app. Fake applications are often disguised as legitimate versions of popular programmes in order to deceive users into downloading and installing the malicious software on their own devices.
After being loaded, fraudulent applications have the potential to steal critical data including passwords, credit card numbers, and other personal information. They may also include harmful code that has the potential to cause harm to the user's device or make it susceptible to infection with malware.

Fake defender

Android Defender is a form of anti-malware software that was developed specifically for use on Android-based mobile devices. By scanning the device for dangerous software and preventing any behaviour that may be considered malicious, it offers security against a wide variety of threats, including malware, viruses, and attempts to hack into a computer system.
Real-time protection, scheduled scans, and the ability to quarantine or delete threats that have been discovered are some of the other functions that the programme could have. Also, certain models of Android Defender may incorporate extra security features, such as protection for the user's privacy, defence against phishing attacks, and spam filtering capabilities.

Fake job offer

A false offer of employment that is issued with the goal of defrauding persons is referred to as a phoney job offer. [Case in point:] Fake websites, emails, or other forms of communication that are made to seem like they came from a real organisation are often used in conjunction with fraudulent employment opportunities. The purpose of these bogus employment offers is either to dupe people into divulging sensitive personal information, such as their Social Security number or bank account information, or to persuade them to part with their money in exchange for said "training materials" or other costs.

Implementation Summary

- Read the CICIDS2017 dataset form the publicly available website. the data is cleaned up and split into training data of 80% and testing data of 20% after the feature extraction process using Min-Max identification etc.
- The data after the min-max estimation need to be fetched to random distribution function. the deep intranet is created with input layer 1x1000, convolution stride layer of 1x10, ReLu layer, filter channel size of 3x3, followed with fully convolution layer of 1x250x4 consequent layers are connected.
- The final layer is the output layer utilized to extract the final class on fake app, fake job offer, android defender, normal etc.

VI. RESULTS AND DISCUSSIONS

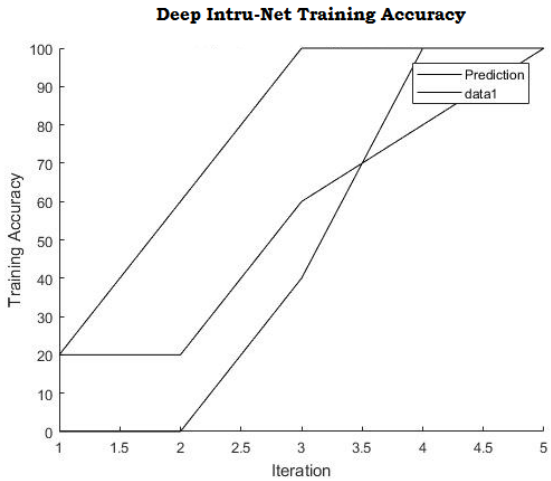

Fig 2. Deep Intru-Net training accuracy

Fig 2.Shows the Deep Intru-Net training accuracy at different iterations are depicted here.

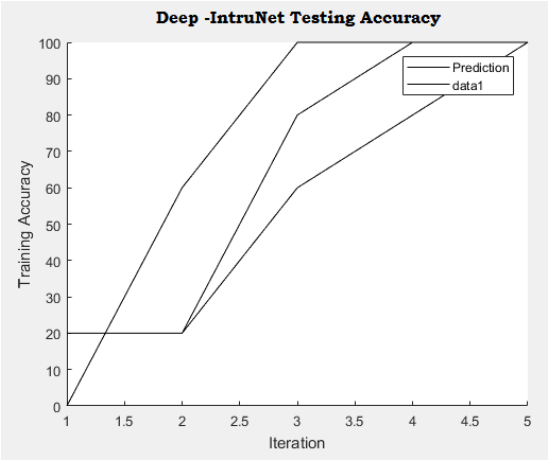

Fig 3. Deep Intru-Net Testing accuracy

Fig 3. Shows the Deep Intru-Net testing accuracy at different ranges of iterations are depicted here.

VII. TABLES

Table 1. Comparison of Proposed approach with Existing methods

S No	References	Methodology	Dataset	Quantitative measures
1	Akhil Krishna et al., 2020	Multi-Layer Perceptron	KUP99	Acc=91.4%
2	Liang, C et al. (2020)	Multi-agent Deep learning	NSL-KDD	Acc=97%
3	Proposed method	Deep Intru-Net	CICIDS2017	Acc=98%

Table 1 explains the different state of art methods comparatively discussed here. [2] using multi layer perceptron achieved 91.4%, [12] using multi agent deep learning approach acheieved 97%. The

The process of intrusion detection is a difficult one that is complicated by a number of obstacles, including the following:

False Positives: Intrusion detection systems often create false positive findings, in which innocuous activity are wrongly categorized as dangerous. These results are referred to as "false positives." This may result in a reduction in trust in the intrusion detection system (IDS), as well as an increase in the burden for security teams, who are required to examine each false positive.

False negatives are another kind of result that may be produced by intrusion detection systems. They occur when potentially harmful behaviour is not uncovered. This might lead to security breaches that are not discovered, which can have severe repercussions for the businesses involved.

Intruders are always coming up with novel ways to avoid being discovered by intrusion detection systems. These methods are referred to as evasion strategies. Attackers, for instance, may make their actions seem to be harmless by manipulating their activities, using encryption to mask their communications, or using stealth measures to avoid being discovered.

Data Volume: Because of the enormous quantity of data that is produced by today's networks, it may be challenging for intrusion detection systems to keep up with all of the data and analyse it in real time.

Variety of Data: Intrusion detection systems need to be able to deal with a variety of data sources, including network traffic, system logs, and application logs. Since the data sources may utilise multiple formats, protocols, and structures, it may be difficult to include all of these aspects into a single study. This may be a difficulty for the reason that it may be difficult to do.

VIII. CONCLUSION

The widespread growth of the internet of things made it possible for a variety of apps to be installed in smart devices, mobile devices, laptops, and other pieces of equipment that are set to allow flexible access to the internet. There have been a lot of people who have benefitted from the dependability of the internet as a common medium. On the same scale of operations, the intrusion assaults pose a danger to the system's level of security. The data that is kept in the cloud has to have some kind of defense against network irregularities. The primary emphasis of the system that is now being presented is the construction of a revolutionary deep learning architecture that features layers that have been optimized to improve performance. The CICIDS2017 dataset is taken into account by the system that is provided. The CICIDS dataset is taken into account by the system as the reference information, and Deep Intru-Net is used to do testing on the architecture that is developed. The dataset is split into training data comprising 80% of the total and testing data making up the remaining 20%. The documented patterns of network irregularities are included in the dataset. The Deep Intru-Net is able to understand the common pattern of anomaly that occurs in the network and recognize when other patterns with the same characteristics arise. The capacity of the system to learn is increased as a result of the better iterations. The accuracy value estimate is what's used to do the performance assessment, and that showed that the suggested network was accurate 98% of the time.

IX. ACKNOWLEDGEMENT

I am grateful to all of those with whom I have had the pleasure to work during this journal and other related projects. Each of the members of my Dissertation Committee has provided me extensive personal and professional guidance and taught me a great deal about both scientific research and life in general to the completion of my project journal titled "**The Deep Intru- Net For Anomaly Detection In Massive Iot Networks**".

REFERENCES

[1] Sheikh Tahir Bakhsh , Saleh Alghamdi, Rayan A Alsemmeari and Syed Raheel Hassan, 2019., in open access journal, SAGE, Soft Comp. in IDS.,
[2] A-Krishna, ALMAA J-Matheiwkutty, DS.-Jacob and HM, "Research on Intrusion Detection & Prevention model Using Deep Learning," 2020 Int. Conf..,((ICESC),(2020,)
[3] A.-Ali and MM.Yousaf-, "., Research entitled Novel triple Intrusion Detec. & safe Gaurd System in SDN..," in IEEE Open-Access Year 2020.,
[4] Zhigang Huang.,, Leii Zhangg., ". Key authentication protocols against smart connected devices.,", IEEE 2019 published.
[5] Rafał-Kozik & Michałl-Chorass., ".,Machine learning tech., Springer –Int. Published 2014.,
[6] M-Islaabudeen, MK. Kavithaa Devi., ". Title ID & PS in Mob. AdHoc-Nws. Against security." Springer published 2020.,
[7] Jin,-YTian, (Z.,-Zhou, M).,& (Li, Z., & Zhang), Z. (2018). ".Home Level Intrusion Detection System using WiFi.," Year 2018, Int. Comp. Conferences.((IWCMC))
[8] (Lin, F., Zhou), (Y., An, X)., (You, I., & Choo), K.R. (2018). ".,Fair Resource Allocation in an IDS for Edge Computing.," IEEE conf. on Secure Consumer electronics Computing., (Year 2018)
[9] Mohammad-Saeid., Mahdavine-jadab., Mohammadreza-Rezvan., Mohammad amin Barekatain., Peyman-Adibia, Payam-Barnaghid Amit., P.Sheth (2018) Science-Direct Published.,
[10] Bh, Deval & Salman, Tara & Samaka, Mohammed & Erbad, Aiman & Jain, Raj. (2016). Feasibility of Supervised Machine Learning for Cloud Security. 1-5. 10.1109/ICISSEC.2016.7885853.
[11] Liang, C.; Shanmugam, B.; Azam, S.; Karim, A.; Islam, A.; Zamani, M.; Kavianpour, S.; Idris, N.B. Intrusion Detection System for the Internet of Things Based on Blockchain and Multi-Agent Systems. Electronics 2020, 9, 1120. https://doi.org/10.3390/electronics9071120
[12] N.-Chaabouni, M.-Mosbahh, A..Zemmari, C.-Sauvignaac and P.-Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," in IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2671-2701, third-quarter 2019, doi: 10.1109/COMST.2019.2896380