REVIEW TECHNIQUE FOR INTRUSION DETECTION MODEL USING RECURRENT NEURAL NETWORKS

Author's Name: [1]Avani Bhoyar, [2]Dr. Vinod Patel

Affiliation: *[1,2] Lakshmi Narain College of Technology, Bhopal, Madhya Pradesh, India (affiliated by AICTE, RGPV)*

E-Mail: bhoyaravani1503@gmail.com

DOI No. – 08.2020-25662434

Abstract

Intrusion detection system (IDS) arrangements with the problematic of fault detection, less accurateness, delays and estimate of attack types. Thus the Review Technique work recommend a data mining based IDS that include the methods that supports to appreciate the network behaviour and predict the attack type precisely after the network traces. IDS are the network monitoring methods that scan the network to recognize the behavioural variations in network. The main purpose of IDS system is to classify the attack situations happened in network and to recognize the nature of attack organised in the network.

Keywords*: IDS, Recurrent Neural Networks*

INTRODUCTION

Currently, there exists an widespread evolution in using Internet in social networking healthcare, e-commerce, bank transactions, and numerous other services. These Internet submissions essential an acceptable level of security and confidentiality. On the additional hand, our computers are below attacks and vulnerable to numerous threats. There is an increasing obtainability of tools and behaviours for attacking and obtrusive networks. An intrusion can be definite as whichever set of actions that threaten the security necessities of a network resource. Intruders have encouraged themselves and conceived pioneering tools that support numerous categories of network attacks. Hence, operative approaches for intrusion detection (ID) have developed an maintaining essential to defend our computers from intruders. In overall, there are two types of (IDS); misapplication detection systems(MDS) and anomaly detection systems(ADS). Maximum profitable IDS employ the misuse approach in which recognized intrusions are deposited in the schemes as signatures. The system explorations network traffics for patterns or consumer behaviours that contest the signatures, if a pattern coordinated a signature; an alarm is elevated to a human security specialist who chooses what action must be occupied based on the type of attack. In such systems, recognized intrusions (signatures) are providing and hand-coded by human specialists based on their extensive experience in classifying intrusions. Current misuse IDS are constructed based on: expert systems which usage a usual of rules to define attacks, signature analysis someplace structures of attacks are captured in audit trail, state-transition investigation which uses state-Anomaly detection, in contrast to misuse detection, can classify novel intrusions. It dimensions models for standard network behavior and customs these profiles to detect novel patterns that meaningfully deviate from them. These apprehensive patterns might signify definite intrusions or could purely be novel behaviors that essential to be additional to profiles. Present anomaly detection systems use arithmetical methods such as multivariate and temporal study to categorise anomalies. Misuse IDS suffer from a quantity of foremost drawbacks, major, recognised intrusions have to be hand-coded by experts. Additional, signature library requirements to be updated when a

innovative signature is exposed, network configuration has been different, or a innovative software version has been connected. Misuse IDS are incapable to detect novel intrusions that do not match signatures; they can only recognize cases that competition signatures. Thus, Tthe scheme fails to classify a new event as an once it , is in detail an intrusion, this is called false negative. On the other hand, present intrusion anomaly detection systems suffer from high proportion of false positives. An extra drawback is that choosing the right set of system features to be measured is ad hoc and based on experience. A collective shortcoming in IDS is that for a huge, complex network IDS can characteristically produce thousands or millions of alarms per day, representing an irresistible task for the security analysts. We organize the paper following format. Section II represent the related work section III represent the proposed methodology, section V conclusion and future work .

RELATED WORK

N. Sokolov et al[1] The capabilities of the measured RNN architectures were established in the IDS problem of ICS. An optimal architecture of RNN was resolute contingent on the definite security level and used subtracting assets.

B. Roy et al[2] This paper concentrations on the binary classification of usual and attack patterns on the IoT network. The new outcomes illustration the efficacy of our proposed perfect through regard . Our proposed BLSTM model accomplishes good accuracy in attack detection. The investigational outcome illustrations that BLSTM RNN is extremely efficient for construction high accuracy intrusion detection model and suggestions a different research methodology

T. Ishitaki, et al[3] In this paper, we present the request of DRNNs for prediction of consumer behavior in Tor networks. To build a Tor server and a Deep Web browser (Tor client) in our laboratory. Then, the customer sends the data surfing to the Tor server expending the Tor network. used Wireshark Network Analyzer to get the data and thenused the DRNNs to type the prediction. The replication consequences illustration that our replication system has a respectable prediction of consumer behavior in Tor networks.

L. O. Anyanwu et al[4] This paper, consequently, suggests a ascendable application-based classical for distinguishing attacks in a communication network expending RNN architecture. Its appropriateness for connected real-time requests and its aptitude to self-adjust to deviations in its input setting cannot be over-emphasized.

V. K. Kukkala et al[5] current a innovative (IDS) called INDRA that uses a gated recurrent unit (GRU)-based recurrent autoencoder to detect anomalies in controller area network (CAN) bus-based automotive entrenched systems. to assess our proposed framework below dissimilar attack situations and similarly associate it through the best known prior all in this area.

N. Mboula et al[6] the consequences illustration that intrusion can be detected in numerous situations whatever the activity of the legit computers of the network. Moreover, the capture device used is based on cheap off-the-shelf components that kinds the deployment onto actual network easy.

INTRUSION DETECTION SYSTEM (IDS)

Vulnerability is a recognized or supposed flaw in the hardware or software or process of a system that revelations the scheme to penetration or unintended revelation of information. Penetration is procurement unauthorized (undetected) access to files and sequencers. Attack is a specific construction or execution of a strategy to transmit out a threat. An attack is effective when a diffusion occurs. Finally, an Intrusion is a conventional of actions intended to cooperation the security goals, specifically; honesty, privacy, or obtainability of a computing and networking source. Figure 1 illustrates the perfect IDS.

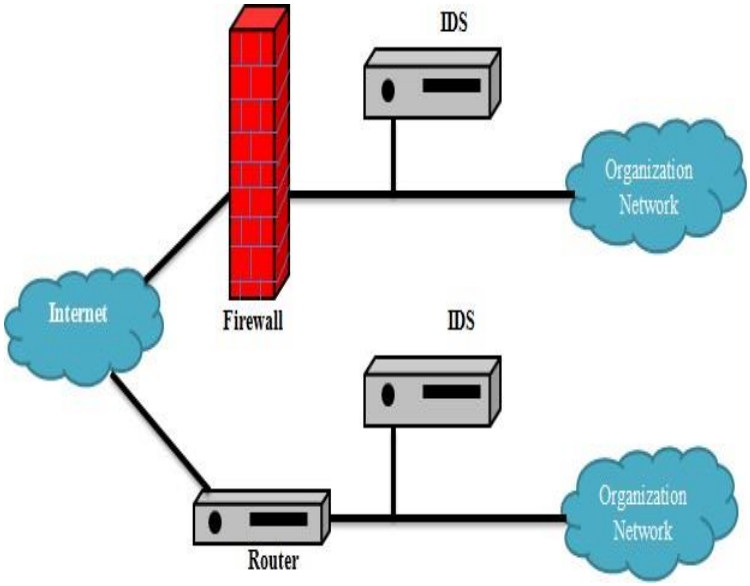

Figure 1: Simple Intrusion Detection Systems

IDS are security systems used to monitor, identify, and explosion malicious activities or policy defilements in computer systems and networks. IDSs are built on the hypothesis that an intruder's behavior will be obviously different subsequently that of a legitimate customer and that several unauthorized actions are quantifiable. Specific of the security violations that would produce irregular patterns of classification convention comprise unauthorized users annoying to obtain into the system, legitimate consumers doing illegal activities, worms and denial of service (DOS) [11]. The objective of intrusion detection (ID) is to recognise, slightly in real time, illegal use, misuse and management of computer systems by composed system insiders and peripheral penetrators [12]. The intrusion detection problematic is attractive added interesting due to the extreme development in computer networks connectivity, the successful technology development and the well-being of detection hackers for hire. IDSs are security systems used to monitor, distinguish and explosion malicious actions or policy obliterations in computer systems and networks. IDSs are created on that an intruder's behavior will be prominently dissimilar from that of a legitimate executive and that recurrent unauthorized actions are detectable. Precise of the security violations that would harvest abnormal patterns of system convention cover unauthorized people difficult to grow into the system, legitimate users responsibility illegal activities, trojan horses, viruses and denial of overhaul [11].

There are frequent behaviors to categorize IDS [13, 14]:

Misuse detection vs. anomaly detection: in misuse detection, the IDS examines the evidence it folds and narrates it to huge databases of attack signatures. Basically, the IDS appearance for a understandable attack that has formerly been documented. Similar a virus detection scheme, misuse detection software is separate as reputable as the database of attack signatures that it customs to associate packets in contradiction of. In anomaly detection, the organization administrator describes the baseline, or usual, state of the networks traffic load, failure, protocol, and typical packet size. The anomaly detector monitors network sections to equate their state to the usual baseline and appearance for anomalies.

Network-based vs. host-based systems: in a network-based system, or NIDS, the separate packets flowing complete a network are analysed. The NIDS can perceive malicious packets that are considered to be overlooked by firewalls simpleminded filtering rules. In a host-based system, the IDS inspects at the action on respectively separate computer or host.

Passive system vs. reactive system: in a passive system, the IDS detect a possible security breach, log the evidence and signal an attentive. In a responsive system, the IDS respond to the apprehensive activity by logging off a user or by reprogramming the firewall to block system traffic from the supposed malicious source. Though they together narrate to network security, IDS varies after a firewall in that a firewall appearance out for intrusions in instruction to stop them from happening. The firewall limits the entrance amongst networks in order to avert intrusion and does not signal an attack from confidential the network. IDS assess a supposed intrusion once it has occupied place and signal an alarm.IDS also watch for attacks that create from inside a system [15].

TYPES OF IDS

Network-based IDS (NIDS): IDS System includes network intrusion detection competences. It examines a traffic passing through the subnet. The traffic ended the network is likened with the database of recognized attacks. The administrator will be sent an alert if the attack is recognized. NIDS monitors the traffic successful done the specific network segment or devices. NIDS gathers the data as the network packets; So it is similarly entitled as packet-sniffer [16].

Host based IDS (HIDS): In Host Intrusion Detection System, the malicious happenings taking place in the only host are scanned. HIDS gathers logs, processes, unauthorized access, changes and uncommon changes in the formation of the system. HIDS is organized on the greatest crucial hosts covering extremely important and openly obtainable information. Such hosts comprise workstations or servers [16].

IDS Techniques: IDS technique

Anomaly detection: The IDS establishes a standard usage pattern and everything that extensively deviates from it becomes flagged is measured as possible intrusion. An anomaly is an occurrence that occurs on frequency less than or better than a standard deviation from statistical opinion of view. Anomalies are recognized by deviations from standard behaviour and any eccentricity from it is flagged as suspect. In this way, novel types of intrusions can be recognized by using novel patterns in the deviation from normal usage or pattern. The drawback of by means of this method is that it raises a actual high false alarm and any formerly hidden behaviour can similarly be considered as an attack. It is intended to uncover the

abnormal patterns of behaviour [17]. The intrusive activity is approved out as a gathering of individual doings and no activity is distinctly anomalous.

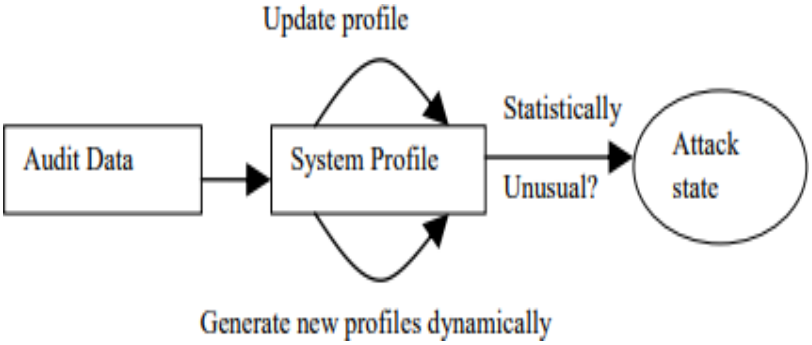

Figure 2: Typical Anomaly Detection

Misuse detection (Signature detection)*:* In this method, there is the dataset in which respectively of the instances is labelled as moreover normal or attack and a learning algorithm is trained on the considered data. As long as the illustrations are labelled suitably; the intrusion detection model can be reinstructed consequently that contain new types of attack. Models of misuse are refined as they are automatically produced. They can detect known attacks with excessive accuracy. Their disadvantage is that they cannot detect novel attacks and they be contingent on signatures extracted by human experts. The recognized patterns of unauthorized behaviour are precisely used to detect and predict following similar attempts. These explicit patterns are called signatures. One instance of signature is for host founded intrusion detection. A precise pattern that matches a helping of network packet can be as simple as a signature for network intrusion detection. For example, an unauthorized action can be designated by header satisfied signatures and/or packet gratified signatures. Some response, alarm, or announcements should be sent to the correct authority relying on the seriousness or robustness of the signature that is activated [17]. A lot of misuse detectors are envisioned to use resolutely lucid signatures that prevent them from classifying abnormalities of collective attacks.

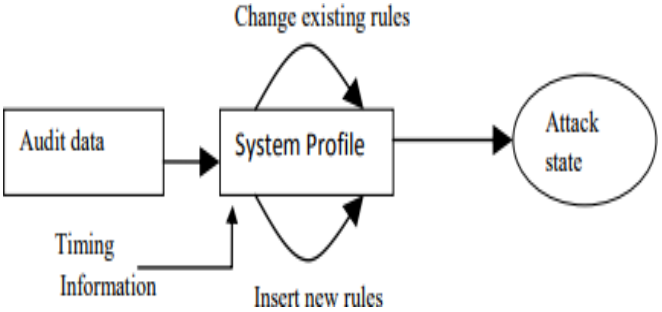

Figure 3: Typical Misuse Detection

Target Monitoring: These system appearances for the alteration of quantified files in its place of enthusiastically searching for anomalies or misuse. This is intended to expose an unauthorized action after it happens to reverse it. The cryptographic hash is calculated beforehand to check for the covert excision of files. This type of system does not need constant monitoring by the administrator, So it is the easiest to implement. It requirements to compute honesty checksum hashes at whatever intervals and on moreover completely files or objective the mission system dangerous files [17].

Stealth Probes : The attacker who selects to transmit out his/her mission for long period is detected by means of this method. For example, an intruder launches an attack to distinguish the vulnerabilities and open ports in the system for a specific period and then he waits for two months and over launches the actual attack. By gathering a diversity of data throughout the system, stealth probes checked for any methodical attacks ended an extended period of time. In an effort to uncover suspicious activity, this technique associations anomaly detection and misuse detection [17].

Hybrid based IDS : Hybrid based IDS associations completely the recompenses of the IDS techniques and overcomes their drawbacks. We have used this method to advance our intrusion detection system. In this IDS, anomaly based method is used to detect new attacks. The signature based method is used to produce the rules for unidentified attacks. The target monitoring and stealth probes are similarly used to classify suspicious activities.

KDDcup99 Dataset and NSL-KDD: The KDD cup99 dataset is the benchmark dataset for IDS. There are three KDD datasets, i.e., KDD modified, through the tremendous growing of the usage of computers over network and development in request running on numerous platform captures the consideration toward network security. This standard adventures security vulnerabilities on completely computer systems that are theoretically difficult and exclusive to solve. Hence intrusion is used as a key to cooperation the honesty, obtainability and privacy of a computer resource. The IDS plays a vital role in detecting anomalies besides attacks in the network. In this work, current data mining perception which is combined with IDS to classify the applicable, hidden data of attention for the user successfully and through less execution time. Classification of Data, The complete proposed algorithm demonstrations better accuracy and concentrated false alarm rate when likened with existing algorithms.

CONCLUSION

We solve the above problematic with better accuracy. Not only in decision making and predicting in numerous domain of security these methods outperforms as associated to traditional methodologies. In this accessible work the data mining method's request in IDS is provided. Moreover the two key issues are targeted for discovery the effective and effective solution. The main aim is to discovery the appropriate features set from the complete dataset. Those assistances to reduce the authorities of data and scale the processing speed of the IDS system. On the next improve the classifier performance for classifying the multiple class data. Expending the two deliberated improvements the a novel data model is proposed for application and design that claims high performance in positions of processing speed and the effective consequences in terms.

REFERENCE

1. N. Sokolov, S. K. Alabugin and I. A. Pyatnitsky, "Traffic Modeling by Recurrent Neural Networks for Intrusion Detection in Industrial Control Systems," 2019 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), Sochi, Russia, 2019, pp. 1-5, doi: 10.1109/ICIEAM.2019.8742961.
2. B. Roy and H. Cheung, "A Deep Learning Approach for Intrusion Detection in Internet of Things using Bi-Directional Long Short-Term Memory Recurrent Neural Network," 2018 28th International Telecommunication Networks and Applications Conference (ITNAC),

Sydney, NSW, Australia, 2018, pp. 1-6, doi: 10.1109/ATNAC.2018.8615294.

3. T. Ishitaki, R. Obukata, T. Oda and L. Barolli, "Application of Deep Recurrent Neural Networks for Prediction of User Behavior in Tor Networks," 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, Taiwan, 2017, pp. 238-243, doi:10.1109/WAINA.2017.63.
4. L. O. Anyanwu, J. Keengwe and G. A. Arome, "Scalable Intrusion Detection with Recurrent Neural Networks," 2010 Seventh International Conference on Information Technology: New Generations, Las Vegas, NV, USA, 2010, pp. 919-923, doi: 10.1109/ITNG.2010.45.
5. V. K. Kukkala, S. V. Thiruloga and S. Pasricha, "INDRA: Intrusion Detection Using Recurrent Autoencoders in Automotive Embedded Systems," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 11, pp. 3698-3710, Nov. 2020, doi:10.1109/TCAD.2020.3012749.
6. N. Mboula and E. Nogues, "IDrISS: Intrusion Detection for IT Systems Security : Toward a semantic modelling of side-channel signals," 2020 28th European SignaL Processing Conference (EUSIPCO), Amsterdam, Netherlands, 2021,pp.735 739,doi:10.23919/Eusipco47968.2020.9287662.
7. A. Prabhu, H. N. Champa and D. Kalasapura, "Network Intrusion Detection Using Sequence Models," 2019 Grace Hopper Celebration India (GHCI), Bangalore, India, 2019, pp. 1-5, doi: 10.1109/GHCI47972.2019.9071806.
8. R. Vinayakumar, K. P. Soman and P. Poornachandran, "Applying convolutional neural network for network intrusion detection," 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, 2017, pp. 1222-1228,doi: 10.1109/ICACCI.2017.8126009.
9. S. Althubiti, W. Nick, J. Mason, X. Yuan and A. Esterline, " Applying Long Short-Term Memory Recurrent Neural Network for Intrusion Detection, " SoutheastCon 2018, St. Petersburg, FL, USA, 2018, pp. 1-5, doi: 10.1109/SECON.2018.8478898.
10. Anand Singh Rajawat Sumit Jain Kanishk Barhanpurkar, Fusion protocol for improving coverage and connectivity WSNs, IET Wireless Sensor Systems, https://doi.org/10.1049/wss2.12018.
11. S. Nayyar, S. Arora and M. Singh, "Recurrent Neural Network Based Intrusion Detection System," 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020, pp. 0136-0140, doi:10.1109/ICCSP48568.2020.9182099
12. A.Kotian, S. Patil, N. Prajapati and Y. Mane, " Realtime Detection Of Network Anomalies Using Neural Network," 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE) , Bengaluru, India, 2020, pp. 240-245,doi: 10.1109/ICSTCEE49637.2020.9276931.
13. S. Sharma and A. S. Rajawat, " A secure privacy preservation model for vertically Partitioned distributed data," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), Indore, 2016, pp. 1-6, doi: 10.1109/ICTBIG.2016.7892653.
14. M. Tan, A. Iacovazzi, N. M. Cheung and Y. Elovici, " A Neural Attention Model for Real - Time Network Intrusion Detection," 2019 IEEE 44th Conference on Local Computer Networks (LCN), Osnabrueck, Germany, 2019, pp. 291-299, doi: 10.1109/LCN44214.2019.8990890.
15. A. K. Desta, S. Ohira, I. Arai and K. Fujikawa, "MLIDS: Handling Raw High – Dimensional CAN Bus Data Using Long Short - Term Memory Networks for Intrusion Detection in In-Vehicle Networks," 2020 30th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 2020, pp.1-7, doi:

10.1109/ITNAC50341.2020.9315024.

16. S. N. Pakanzad and H. Monkaresi, " Providing a Hybrid Approach for Detecting Malicious Traffic on the Computer Networks Using Convolutional Neural Networks", 2020 28th Iranian Conference on Electrical Engineering (ICEE), Tabriz, Iran, 2020, pp. 1-6, doi:10.1109/ICEE50131.2020.9260686
17. Y. Peng, " Application of Convolutional Neural Network in Intrusion Detection,''2020 International Conference on Advance in Ambient Computing and Intelligence (ICAACI), Ottawa, ON, Canada, 2020, pp. 169-172, doi: 10.1109/ICAACI50733.2020.00043.
18. A. A. Abdul Lateef, S. T. Faraj Al – Janabi and B. Al – Khateeb, " Hybrid Intrusion Detection System based on deep learning ,'' 2020 International Conference on Data Analytics for business and industry : way towards a Sustainable Economy (ICDABI), Sakheer, Bahrain, 2020, pp. 1-5, doi: 10.1109/ICDABI51230.2020.9325669.
19. Rajawat A.S., Upadhyay P., Upadhyay A. (2021) Novel Deep Learning Model for Uncertainty Prediction in Mobile Computing . In : Arai K., Kapoor S., Bhatia R. (eds) Intelligent Systems and Applications. IntelliSys 2020. Advance in Intelligent Systems and Computing , vol 1250. Springer , Cham. https://doi.org/10.1007/978-3-030-55180-3-49
20. S. S. Swarna Sugi and S. R. Ratna, " Investigation of Machine Learning Techniques in Intrusion Detection System for IoT Network '', 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 1164-1167, doi: 10.1109/ICISS49785.2020.9315900.