Enhancing Intrusion Detection System In Computer Networks Using AI Techniques

Shaik Azaruddin[1], T.P.Anithaashri[2]

[1.] *UG Scholar, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, azaruddin14311@gmail.com*

[2.] *Associate Professor, Institute of Computer Science and Engineering, Saveetha School of Engineering,Saveetha institute of Medical and Technical Sciences, Chennai, anithaashritp.sse@saveetha.com*

Abstract :
Machine learning techniques are being widely used to develop an intrusion detection system (IDS) for detecting and classifying cyberattacks at the network-level and the host-level in a timely and automatic manner. However, many challenges arise since malicious attacks are continually changing and are occurring in very large volumes requiring a scalable solution. There are different malware datasets available publicly for further research by cyber security community. Due to the dynamic nature of malware with continuously changing attacking methods in the computer network, the malware datasets available publicly are to be updated systematically and benchmarked with the proper security. The enhancement needs to rule in identifying the intrusions in the system so as to provide the secure data accessibility through computer network using various intelligence techniques with the help of multiple sensors in the communication link.

Keywords:Anonymous, Intrusion, network

1. INTRODUCTION :

Intrusion Recognition method is a software which is utilised for observing network as well as securing from attacker. Due to tremendous change in these modern technology areas of new applications has been introduced. Mean while areas in Commercial business, finance,industrial, protection and health safety sectors the Local area network as well as the wide area network apps has been emerged. Areas of applications had done the network which resembles an achievement for improper security and unprotected security for organisation. Intruders or attackers utilized inner methods of organisation to grab info as well as cause major problems like Issues of software, Time lapse error, System protection to fixed version. In the internet accessibility, various novel technologies and next generation advancement need to address various new attacks causes to the systems. To enter into various system, they would like to do the following activities like injecting virus, hacking the main servers. Firewall method is famous security methods as well as which is utilized to safe closed network to open network. IDS are utilised in network which relates some undergoing tasks like fraud activities etc. can be viewable easily and accessibility to the data through secured network.

2. LITERATURE REVIEW:

Because of effect of organised sending atmosphere, serious limitations in control along with less hardware material, as well as absence of unified organization in the board, remote sensor systems (WSNs) are incredibly powerless against malevolent [3]assaults planned for directing and different angles. Confronting these issue, we introduce novel faith-mindful directing convention for WSNs which joins variety of attributes (TRPM) of sensor hubs as far as correspondence, information, vitality, and suggestion. The introduced faith project depends modified slider time windows containing assault recurrence to encourage the disclosure of noxious practices [5] of aggressors. Joined with viable directing identification as well as upkeep convention, the exhibition of answer is tried with a arrangement of reenactment tests. Broad outcomes uncover that a normal parcel move pace of TRPM is expanded with 27% and time utilization on the steering version is abbreviated by about 18.9%. Wireless Sensor Networks are mostly utilised in producing apps for investigation, observing, borderline protection, intrusion[2] recognition. From the network nodes, applications are essential for protected transmission of data. From various types of strikes critical data[7] app faces, wrong data involved strikes are highest critical damaging and dangerous. The preventive measures of those are major thing when forming critical data[9] remote sensor network apps. Analysers has proposed [17] that Encoding techniques such as Blowfish, AES algorithm[13] for control measures. These Encoding methods[16] are useful rapidly rises calculation difficulty of node as well as contains of energy on the order of WSN[11] of another answer for wrong data involved strikes counter measure. Introduced project targets on utilizing trust framework[13] of each hub to recognize malignant as well as non-malevolent[14] hubs as well as utilize just confided in hubs to advance the parcel to goal [1] along these lines by aversion FDI assaults. Reproducing is done by assistance of Network Simulator 2 (NS2). Final outcomes gives vitality utilization is low in introduced plan contrasted with encoding system.

3. PROPOSED SYSTEM :

The proposed systems starts with the segments of assaults identification which presentsprocessing of data are gathered by sensors to distinguish assaults. The Database modules stores the entire data to have detection over the information module contains the information related to the detection.Detector module is a device that is used to detect the intrusion with an notification provided by the intelligence tools. Then the counter act will be taken place and it goes to the system info module.Network and host are the sensors of two kinds are utilized in intrusion recognition methods. Those sensors are intended to gather data related to information parcels are transferred in Information Server partition, where sensor recognizes the intrusion.

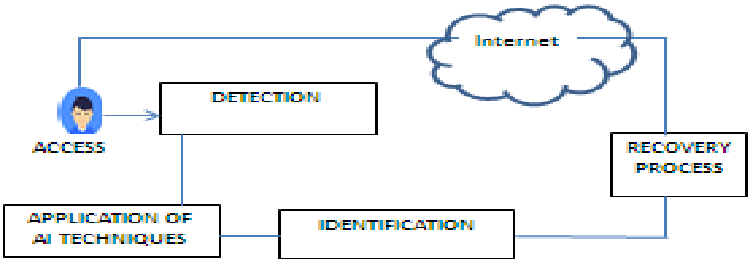

Figure 1.OVERVIEW ARCHITECTURE

These servers are introduced by host sensors as well as are intended to gather data which relates information bundles that are collected with sensor. Data is gathered by system as well as sensors of host, it will be broke down by interruption recognition framework to recognize assaults of violators. Information can be completed by two fundamental gatherings of strategies - signature-based . The architecture diagram specifies the working function of the proposed system. It starts with detecting the intrusion using sensor and other system, then by applying proper AI techniques it can be identified the type of the anamolyness and then get in to the process of recovery and thus provides the solution to the exiting problem.

The Final outcome of the assessment has been arrived by Measurements which are utilized to assess the methods are Detection Rate(DR),False Alarm Rate(FAVR)as well as precision. Final generated outcomes presents that initiated strategy Fuzzy Logic – Support Vector Machine (FL-SVM) beats other cross breed strategies as far as Detection Rate (DR), precision and False Alarm Rate (FAR).

4. CONCLUSION :

At present Intrusion recognition is getting attention from research authority as well as from Large Organisations. Depends upon the introducedanalysis which are represented with various solutions in which the system has declared the present state-of-the-art of IDS with an improvisation in performing the task in a stipulated time. This analysis too gives importance to the past duties as well as retells previous work and present works medication frequently. Every methods have pros and cons. It is strongly opposed that no standards are utilised totally to protect opposition to PC network Intrusion. It has been proposed with every attaindetection of various upgrades which can be utilised as definite answer to current scenario in network accessibility. If it comes under expense criteria, it is very hard to sustain the PC methods as well as networks which leads to various attacks. Methods which are chosen relies upon determinations of the kind of peculiarity that the methods should confront sort as well as conduct of the information, nature wheremethods are functioning in an efficient way to achieve the specific task.

REFERENCES:

[1] T.P.Anithaashri, G. Ravichandran, R.Baskaran, Software Defined Network Security enhancement using Game Theory, Elsivere COMNET, vol157, pp:112-121, 2019

[2] T.P.Anithaashri, G. Ravichandran, et.al. Secure Data Access Through Electronic Devices Using Artificial Intelligence, ICCES, 2018.

[3] George D. O'Mahon, Philip J. Harris, Colin C. Murphy “Analyzing the Vulnerability of Wireless Sensor Networks to a Malicious Matched Protocol Attack” IEEE 2018.

[4] Berjab, HieuHanh Le, Chia-Mu Yu, Sy-Yen Kuo, Haruo Yokota “Abnormal-Node Detection Based on Spatio-Temporal and Multivariate-Attribute Correlation in Wireless Sensor Networks” IEEE 2018.

[5] Networks AmjadMehmood, Akbar Khanan, Muhammad Muneer Umar, Salwani Abdulla, KhairulAkramZainolAriffin, Houbing Song “Secure Knowledge and Cluster-Based Intrusion Detection Mechanism for Smart Wireless Sensor Networks” IEEE 2018.

[6] Haibin Zhang, Jiajia Liu, Nei Kato “Threshold Tuning-Based Wearable Sensor Fault Detection for Reliable Medical Monitoring Using Bayesian Network Model” IEEE 2018.

[7] Cong Pu, SunhoLim,“A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation” IEEE 2018.

[8] T.P.Anithaashri, R. Baskaran, Enhancing Multi-user Network using sagacity dismissal of conquered movements, International Journal of American Scientific Publishers, 2016 pp:69-78

[9] ParveenSadotra and Chandrakant Sharma. A Survey: Intelligent Intrusion Detection System in Computer Security. International Journal of Computer Applications 151(3):18-22, October 2016

[10] A. Araujo, J. Blesa, E. Romero, D. Villanueva, “Security in cognitive wireless sensor networks. Challenges and open problems”, EURASIP Journal on Wireless Communications and Networking, February 2012.

[11] A. Abduvaliyev, S. Lee, Y.K Lee, “Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks”, IEEE International Conference on Electronics and Information Engineering, Vol.2, pp. 25-29, August 2010.

[12] M. Ali Aydın *, A. HalimZaim, K. GokhanCeylan “A hybrid intrusion detection system design for computer network security” Computers and Electrical Engineering 35 (2009) 517–526.

[13] G.Li, J.He, Y. Fu. “Group-based intrusion detection system in wireless sensor networks” Computer Communications, Volume 31, Issue 18 (December 2008)

[14] A. Becher, Z. Benenson, and M. Dorsey, \Tampering with motes: Real-world physical attacks on wireless sensor networks." in SPC (J. A. Clark, R. F. Paige, F. Polack, and P. J.Brooke, eds.), vol. 3934 of Lecture Notes in Computer Science, pp. 104{118, Springer, 2006.

[15] I. Krontiris and T. Dimitriou, \A practical authentication scheme for in-network programming in wireless sensor networks," in ACM Workshop on Real- World Wireless Sensor Networks, 2006

[16] Michael Brownfield, “Wireless Sensor Network Denial of Sleep Attack”, Proceedings of the 2005 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY.

[17] K. Akkayaand M. Younis, ―A Survey of Routing Protocols in Wireless Sensor Networks, ‖ in the Elsevier Ad Hoc Network Journal, Vol. 3/3 pp. 325-349, 2005

[18] I. F. Akyildiz et al., “Wireless Sensor Networks: A Survey, “Elsevier Comp. Networks, vol. 3, no. 2, 2002, pp. 393–422