Journal of Engineering Sciences
Vol 11, Issue 11, NOV/2020
ISSN NO:0377-9254

Detection of Cyber anomaly Using Fuzzy Neural networks

[1]P.Padma, [2]Vadapalli Gopi, [3]M.Kiran Kumar

[1]Associate Professor, Department of Information Technology, Guru Nanak Institutions Technical Campus
[2]Assistant Professor, Department of CSE, Sri Vani Engineering College, Chevuturu, Krishna District
[3]Assistant Professor, Department of Information Technology, Guru Nanak Institutions Technical Campus
Ibrahimpatnam, Hyderabad

ABSTRACT:

The fuzzy neural networks belong to the Hybrid structured family which perform several acts in various contexts pf pattern classification which includes the detection of abnormal or anomalous behaviour. In this paper it is clearly presented the application of artificial intelligence on the basis of association between empowering artificial neural network and fuzzy logic to detect anomalies in the data transmission in a computer network and when cyberattacks take place. Apart from verifying accuracy of the fuzzy model, the rules were obtained through a deep understanding and imparting knowledge from the massive datasets to make an expert system. The rules create an intelligent system in high-level languages with a high accuracy level of detention of anomalies in data transaction.The huge clusters and large volume of data from different sources has created a lot of new service and also precautions, these data circulating in digital world promotes strategies in making the performance more effective with ensuring that they are well diagonised by its team and stackholders. The distinct evolution of scientific resources rains the change of several situations and promoting e-commerce, online businesses etc, many companies have also estimated the power of internet and making business online, even the prestigious US and Brazilian elections have used the digital media to share information. This is the context of high volumes of data on the internet and usage has been more vivid and technologies that support internet and online business have increased to this evovlved includes more amount of security and privacy concerns. Many precautions and steps shall be taken by the users and the corporates so that their data is safe and doenst includes any malicious concerns.This paper contributes to the hybrid model with a high degree os assessment in prediction and detection of anomalous behaviours using the set of rules of AI which are tolerant of constructing an anti threat system. Knowledge gained from fuzzy rules in this process creates an expert system in detection of anomalous behaviour. It is simple to to understand fuzzy relations with the metrics given by them from low to high.

INTRODUCTION:

Proposed system:

Proposed Detection of Cyber Invasions through Detection of Anomalies through Hybrid Models and the Creation of Expert Systems

The hybrid system proposes to use fuzzy neural networks and train them with the database that determines patterns of anomalies. Through these standards, the model learns the trends and characteristics of the database, allowing in addition to pattern classification, create an expert system based on fuzzy rules. The model will have four dimensions (service, duration, bytes received, bytes sent) according to the formatting of bases for the detections of anomalies. These four features will be combined according to equally spaced membership functions. In an example with two pertinence functions for each input of the model, eight Gaussian neurons are generated in the first layer and consequently 16 fuzzy logical neurons in the second layer. Therefore N = 4, M = 2, L = 16. These 16 fuzzy neurons represent the union of fuzzy rules of the first layer.It follows then that L = NM. The methodology is synthesized as demonstrated in Algorithm 1. It has two parameter:

The hybrid system to automate fuzzy nuural networks and coach them with the data that determine anomalies. Though these system are created in a way that is used to learn the trends and characterises the database in pattern classification, creating expert system based on fuzzy rules. This hybrid model has 4 metrics like bytes received, bytes sent, duration, service.

These features will be incorporated with equal spacing functions. then, 8 gaussian neurons are reported in the primary layer and 16 fuzzy logical neurons in the territory layer.

Eg: N=4, M=2, L=16 – primary layer and L=N*M is the territory layer.

Algorithm 1: Fuzzy Neural Network for anomaly detection -FNN training

Step -1: Define the number of membership functions, M.

Step -2: Calculate M neurons for each characteristic in the first layer using ANFIS.

Step -3:Construct L fuzzy neurons with Gaussian membership functions constructed with center and σ values derived from ANFIS.

Step -4: Define the weights and bias of the fuzzy neurons randomly.

Step -5: Construct L fuzzy logical neurons with random weights and bias on the second layer of the network by welding the L fuzzy neurons of the first layer.

Step -6: For all K input do

Step -6.1: Calculate the mapping zk (xk) using andneurons end for

Step -7: Estimate the weights of the output layer using Equation

Step -8: Calculate output y using leaky ReLU using Equatiojn (1).

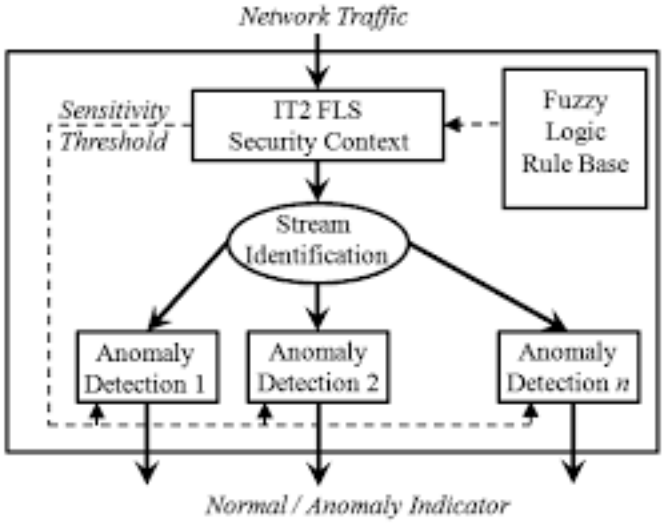

Fig: Proposed system architecture

Anomaly Detection Test:

Dataset Uses the dataset used for the experiments in this paper was originally provided in the KDD Cup 1999 and is currently available in the main data repository for machine learning. It contains 41 attributes (34 continuous and seven categorical) [20]. However, they are reduced to 4 attributes (service, duration, bytes received, and bytes sent) because these attributes are considered the most basic attributes where only the service is categorical [21]. Using the service attribute, the data is divided into http, SMTP, FTP, FTP data, other AI 2020, 1 105 subsets [22]. That allows distinct types of attacks to be verified by intelligent algorithms. Here, only HTTP service data is used. Since the values of the continuous attributes are

concentrated around 0, we transform each value into a value far from 0, by y = log (x + 0.1). The original dataset has 3.925.651 attacks (80.1%) of 4.898.431 records [23]. A smaller set is forged by having only 3.377 attacks (0.35%) of 976.157 records, where the logged-in an attribute is positive. From this forged dataset, 567.497 HTTP service data is used to construct the HTTP dataset .The database was selected precisely with the main feature of a cyber attack: a large volume of requests with attacks entered together with them. Thus, protection systems are overloaded and often miss attacks that can compromise system integrity. Therefore, a system that acts dynamically in identifying these patterns, especially as assertively as possible, is necessary for maintaining system integrity. The database provided by the KDD Cup has the characteristics of large-scale attacks as the number of requests is exceptionally high. Moreover, in these requests, there are less than 2% of malicious attacks. Therefore, the database meets the anomaly detection criteria (when the database is hugely unbalanced about its labels) and the large scale criteria for having more than millions of requests.

- accuracy = TP + TN TP + FN + TN + FP (12)
- sensitivity = TP TP + FN
- speci f icity = TN TN + TP
- AUC = 1 2 (sensitivity + speci f icity)
- where, TP = true positive, TN = true negative, FN = false negative and FP = false positive.

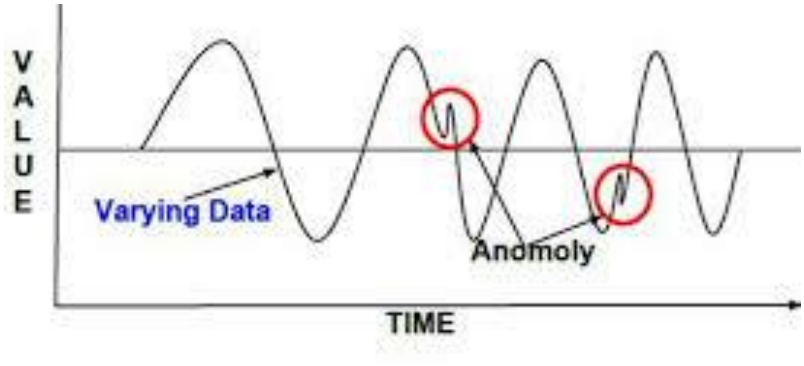

Fig: Anomoly detection using AI tools

Expert Systems in Detecting Anomalies in Cyberattacks through Fuzzy Rules

The linguistic characteristics adopted for the formation of the rules were defined in consultation with experts in the field. Shows the ANFIS structure formed with one of the results of the 30 replicates performed with the model. The three dimensions were shaped using equally spaced Gaussian membership functions. Here it can see the influence of fuzzy inputs for the fuzzy inference system that will generate rules based on dataset knowledge.
In fuzzy rules, it is possible to identify the decision space of the model by the duration of a request, the number of bytes received and sent. Large-scale cyber attacks work with the methodology of overloading data servers to make them more susceptible to attack. Thus, it is possible to define the number of elements evaluated in each dimension of the problem for FNN decision making. Likewise, the graphic knowledge of a fuzzy neural network can be presented linguistically and relationally allowing anyone interested in protecting computer systems to understand when a cyber-attack can occur, even those who are not profoundly knowledgeable.

of artificial intelligence. So this is the most significant advantage of the model because it allows the clear and straightforward dissemination of implicit knowledge in a database. In these relationships obtained, it can be seen that the highest correlation between the identification of cyber-attacks is linked to the reduction of the duration of requests tied mostly to a low amount of bytes received.

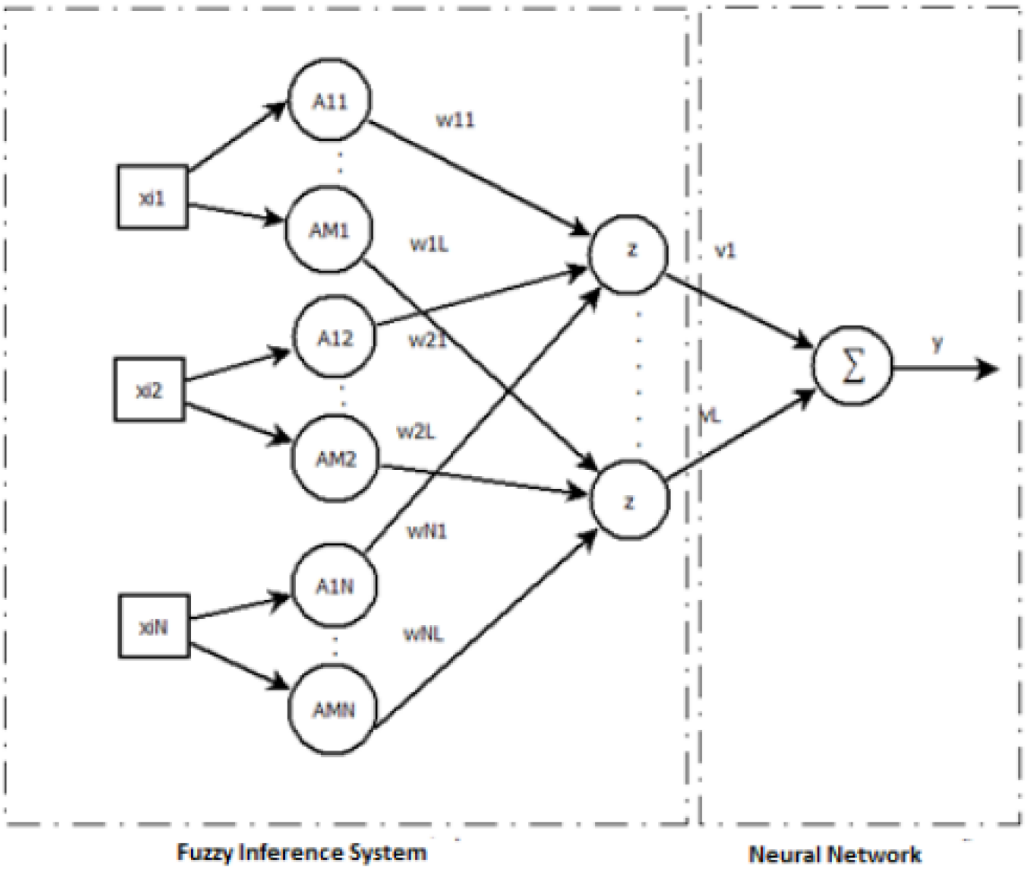

Fig: Detection of cyber anomalies in large scale

CONCLUSIONS:

After the presented results, we can conclude that the fuzzy neural networks used in this paper can act as unique identifiers of anomalies. Because it is an unbalanced problem or more than 99% of the samples are of one category, the model behaved efficiently to identify the anomalies, and in most of the trials, it has found all of them.

However, it should be noted that even with the high execution time of the algorithm, the results of the model proposed in this paper were the best in the evaluation indexes, adding to the results of the possibility of obtaining knowledge about the attacks and improving the results. Protection devices that operate on cyber threat systems with knowledge extracted from the dataset. Fuzzy rules can be easily implemented in information systems that have logical programming, as can electronic devices that can also be programmable. The model can be seen as an approach to knowledge management in Big Data since it can extract knowledge from a database and turn it into a set of linguistic rules, more accessible to interpret by people who do not are directly linked to the computer science area. This type of approach assists in the dissemination of intelligent techniques and can contribute to advances in science and the prevention of anomalies.

FUTURE WORK

1.Attempts will be made to suitably modify existing algorithms or to develop new ones using Fuzzy

2.Set theory based on intrusion detection techniques for anomaly based intrusion detection. New algorithms developed will be evaluated with benchmark datasets and their performances will be compared empirically with the existing algorithms.

REFERENCES

[1]AgustınOrfila, Javier Carbo, and Arturo Ribagorda (2006), ―Effectiveness evaluation of data mining based IDS‖, CS department, Carlos III University of Madrid Aleksandar Lazarevic, Vipin Kumar, Jaideep Srivastava (2003) ―Intrusion Detection: A Survey‖,Springer link, chapter 2, pp.21-78

[2]Rajdeep Borgohain(2012) , ― FuGeIDS: Fuzzy Genetic paradigms in Intrusion Detection Systems‖ ,IJANA, Volume:03 Issue:06 ,ISSN : 0975-0290, pp.1409-1415

[3]CERT® Advisory CA-2003-04 MS-SQL Server Worm,(2003) http://www.cert.org/ Advisories /CA-2003-04.html

[4]D, Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford and N. Weaver(2003), ―The Spread of the Sapphire/Slammer Worm, http://www.cs.berkeley.edu/~nweaver sapphire‖

[5]Dat Tran, Wanli Ma, Dharmendra Sharma and Thien Nguyen (2007), ―Fuzzy Vector Quantization for Network Intrusion Detection‖, in the proceedings of IEEE International Conference on Granular Computing ,San Jose, California, USA

[6]Gao Xiang, Wang Min, Zhao Rongchun(2005), ―Applying Fuzzy Data Mining to Network Unsupervised Anomaly Detection‖, ISCIT 2005, IEEE Computer pp. 1249-1253

[7]Georgios P. Spathoulas and Sokratis K. Katsikas (2010) , ―Reducing false positives in Intrusion Detection Systems‖ , Elsevier , computers & security journal 29 pp.35 – 44

[8]H. Adeli and A. Karim (2005), ―Wavelets in Intelligent Transportation Systems‖, John Wiley &Sons UK

[9]Herv´e Debar and JouniViinikka (2005), ―Intrusion Detection: Introduction to Intrusion Detection and Security Information Management‖,FOSAD, pp. 207-236

[10]J.R. Winkler(1990), ―A Unix Prototype for Intrusion and Anomaly Detection in Secure Networks‖, In Proceedings of the 13th National Computer Security Conference, Baltimore, MD

[11]J.R. Winkler and L.C. Landry(1992), ―Intrusion and Anomaly Detection‖, ISOA Update, In Proceedings of the 15th National Computer Security Conference, Baltimore, MD

[12]K. Sequeira and M. Zaki, ADMIT (2002), ―Anomaly-base Data Mining for Intrusions‖, Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Edmonton, Canada

[13]K. Yamanishi and J. Takeuchi(2001), ―Discovering Outlier Filtering Rules from Unlabeled

Data‖, In Proceedings of the Seventh ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, CA

[14]K. Yamanishi, J. Takeuchi, G. Williams and P. Milne(2000), ―On-line Unsupervised Outlier Detection Using Finite Mixtures with Discounting Learning Algorithms‖, In Proceedings of the Sixth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Boston, MA, pp.320-324

[15]Kai Hwang, Ying Chen, and Min Qin (2007), ―Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes‖, IEEE transactions on dependable and secure computing, vol. 4, no. 1, pp.41-55

[16]Lata Jadhav, Prof.C.M.Gaikwad (2014),―Implementation of Intrusion Detection System using

GA‖, ISSN:2393-9842,Vol.1 Issue.1

[17]Mohammad SanieeAbadeh_, Jafar Habibi, ZeynabBarzegar, and MunaSergi (2007) , ―A parallel genetic local search algorithm for intrusion detection in computer networks‖, Elsevier , Engineering Applications of Artificial Intelligence 20 ,pp.1058–1069

[18]Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu NaserBikas(2012), ―An

Implementation of intrusion detection system using genetic algorithm‖, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2,pp.109-120
[19]Ming-Yang Su, Gwo-Jong Yu and Chun-Yuen Lin(2009) , ―A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach‖ , Elsevier , computers & security 28 , pp. 301 – 309
[20]M. Kiran Kumar, Dr. K. Bhargavi. An Effective Study on Data Science Approach to Cybercrime Underground Economy Data. Journal of Engineering, Computing and Architecture.2020;p.148.
[21] M. Kiran Kumar , S. Jessica Saritha. AN EFFICIENT APPROACH TO QUERY REFORMULATION IN WEB SEARCH, International Journal of Research in Engineering and Technology. 2015;p.172.
[22] M KIRAN KUMAR, K BALAKRISHNA,M NAGA SESHUDU,A SANDEEP. Providing Privacy for Numeric Range SQL Queries Using Two-Cloud Architecture. International Journal of Scientific Research and Review. 2018;p.39
[23] K BALA KRISHNA, M NAGASESHUDU, M KIRAN KUMAR. An Effective Way of Processing Big Data by Using Hierarchically Distributed Data Matrix. International Journal of Research.2019;p.1628
[24]Mei-Ling Shyu, Zifang Huang, and Hongli Luo(2009), ‖Efficient Mining and Detection of Sequential Intrusion Patterns for Network Intrusion Detection Systems‖, Machine Learning in Cyber Trust, , Volume . ISBN 978-0-387-88734-0. Springer-Verlag US, pp. 133-154
[25]N. Ye and Q. Chen(2001), ―An Anomaly Detection Technique Based on a Chi-Square Statistic for Detecting Intrusions Into Information Systems‖, Quality and Reliability Engineering International, vol. 17, 2, pp. 105-112