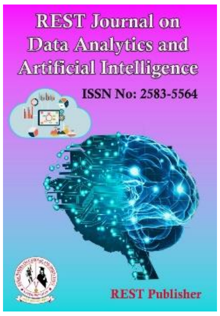
REST Journal on Data Analytics and Artificial Intelligence

Vol: 2(1), March 2023

REST Publisher; ISSN: 2583-5564

Website: http://restpublisher.com/journals/jbab/

DOI: https://doi.org/10.46632/jdaai/2/1/13



Network based Intrusion Detection System using the SPSS Method

[1]S. Siva Shankar, *[2]Vimala Saravanan, [2]M. Ramachandran, [2]R. Sangeetha

[1]KG Reddy College of Engineering and Technology, Hyderabad, Telangana, India.

[2]REST Labs, Kaveripattinam, Krishnagiri, Tamil Nadu, India

*Corresponding Author Email: vimala@restlabs.in

Abstract. *An invasion detection system (NIDS) that makes use of networks can spot malicious activities on a network. For NIDS to inspect each and every packet of communication, including unicast traffic, invalid network access is often required. Along with being small structures that don't block traffic, NIDS are able to keep an eye on usernames and passwords, check for any signs of odd activity in the file integrity logs, port logs, mysql database file storage, etc. and alert the part of implementing as necessary. Since NIDS keeps an eye on live data, it can spot problems as they happen. On the other hand, HIDS uses historical data to identify skilled hackers who employ cutting-edge methods that are difficult to detect in real-time. A monitoring system called an intrusion notification system (IDS) looks for abnormal activity and sends out alarms when it does. A Counter Terrorism Center (SOC) analyst senior incident handler can look into the issue and take the necessary steps to resolve the threat based on these notifications. Every incoming packets are read by an NIDS, which scans them for any anomalous activity. Depending on the gravity of the danger, steps can be taken, such as alerting system administrators or preventing the initial IP address from connecting to the network. In the past decades, due to developments Increased use of networking techniques and internet, digital. Contacts entered into everything that happens on the world market. The hacker penetration attempts are taking place in parallel with these advances. Networks are expanding as well. Without permission, they attempted to modify some network data or increase network traffic in order to launch a denial-of-service attack. Intrusion prevention systems (IDS) are also favoured, especially for detecting malicious within a network system, even though a firewall may appear like an useful solution to avoid this type of attack. Machine learning algorithms have helped IDS become more successful in recent years, depending on the consequences of the training/learning process. Knowing what is important is very difficult and the learning algorithm is fast according to the problem Type. The complexity of the task, the size of the data sets, the number of nodes, the network design, the intended error rate, etc. all affect the choice of algorithm. Examine several network training functions in artificial neural networks with numerous layers created to provide effective intrusion detection systems. test outcomes The study provides evidence of the usefulness of the approach. Considering their speed and true-positive detection rates Death Penalty. SPSS statistics is multivariate analytics, business intelligence, and criminal investigation data management, advanced analytics, developed by IBM for a statistical software package. A long time, spa inc. Was created by, IBM purchased it in 2009. The brand name for the most recent versions is IBM SPSS statistics. Network Security, Intrusion Detection System, Neural Networks and Training Functions. The Cronbach's Alpha Reliability result. The overall Cronbach's Alpha value for the model is .860which indicates 86% reliability. From the literature review, the above 50% Cronbach's Alpha value model can be considered for analysis. Emotional Intelligence the Cronbach's Alpha Reliability result. The overall Cronbach's Alpha value for the model is .860which indicates 86% reliability. From the literature review, the above 50% Cronbach's Alpha value model can be considered for analysis.*

Keywords: *Network Security, Intrusion Detection System, Neural Networks and Training Functions.*

1. INTRODUCTION

Intrusion detection is the process of spotting intruders' attacks on information systems. These actions, which are sometimes known as incursions, are meant to obtain unrestricted control over a computer system. External or internal intruders both exist. Those who have a modicum of valid access to the network but try to abuse unauthorized powers by elevating their access privileges are known as internal invaders. Users just outside of the target network are considered external intruders when they attempt to access system data without authorization. A typical IDS involves sensors, a reporting system, and an analysis engine. at different hosts or locations inside the network, sensors are placed. They are tasked with gathering host or network data, including traffic information, packet contents, service requests, windows system calls, etc file system modifications [1]. The use of Internet technology has increased recently in a variety of fields, including social networking, online application/registration, online auctions, and financial activities. Nonetheless, many computer systems are frequently breached by hackers due to lax computer system security, particularly using limitation of service or disseminated denial of service assaults. The usage of firewalls and some type of access control mechanism is one of the most popular intrusion detection/prevention strategies. They fall short, however, if the hacker is within the network or if he is knowledgeable and employs novel attack techniques [2]. The primary achievement of this research is a comprehensive evaluation of the literature on network-based information and a determination of which datasets meet which dataset characteristics. The emphasis of this research is on attack scenarios inside data sets and the connections between them. As new sources of data transfer outside traditional data sets, we also briefly discuss traffic generator and data sources and offer some observations and suggestions. This survey has the major benefit of establishing a collection of data range characteristics that can be used to compare the various data sets that are now available and to determine which data sets are best suited for certain evaluation scenarios. We also built a website 1 which thus lists all the datasets as well as data repositories described above and plan to maintain this website [3]. Competitive network-based detection technologies such as Net Ranger and Real Secure progressed from single-connection monitor techniques to distributed designs. Sensors and directors are the two different sorts of modules that make up Net Ranger systems for detection of intrusions. In order to identify network-based assaults, sensors are network monitors that examine traffic on the network on a network segment and record data produced by Cisco routers. A module in charge of running the Censor Board is called a Director. Large networks can be managed by directors that can be set hierarchically. Network algorithms, system users, and managers are components of an intrusion detection system that is really secure. Network monitors called network engines compare the traffic on a communication link to attack signatures [4]. How to determine the number of colonies in advance; how to initialise the Center of Gravity for Clusters (COGs); and how to determine the maximum radius of clusters are the three most frequent issues with intrusion detection clustering approaches. Low effectiveness of the approach may be caused by improper parameter selection. A cluster is also described by its COG as well as sample distance from the COG in centroid-based clustering algorithms, which gives the clusters hypersphere-like geometries in a given input space [5]. IDS Implementation in MANET Related Intrusion Detection Algorithms. The authors claim that depending on the fundamental idea employed to identify the assault, these IDS technologies can be divided into many types. These rules, statistics, heuristics, signatures, levels, popularity scores, or paths employed can be examples of these ideas. These methods are then further divided into hybrid, hybrid-based, anomaly detection, misuse, and signature-based methods. Authors have suggested additional classification criteria, including attack types, real-time/offline, and radar detector (scalability, reliability, and timeliness)[6]. detection of applications area intrusions. This dataset aims to assess several intrusion detection technologies that have been presented. This dataset is not appropriate for formal language SVM input because it is simply a categorised dataset with the name normal or attack name. We transformed this information into a common SVM input format. 4,898,431 instances make up the entire training set, while 311,029 instances make up the entire 10% labelled test set. From the training set, we randomly selected the knowledge set and the testing dataset. Yet, the training dataset is different from the learning set. inside the test set, we also randomly selected sub-test sets [7]. a model for intrusion detection that classifies attacks properly. Our model should also use less computational power to do the classification and offer a lower rate of false alarms and a better detection rate for occasional and frequent attacks. When IDS are employed in machinery control systems that operate vital infrastructure, where accurate and prompt notification of cyberattacks is essential, the latter trait is especially significant. We first summarise the suggested framework for networks of the Internet of Things. New, pertinent works that have just been published have been presented as well as critically reviewed [8]. Systems for network-based intrusion detection and related research. The suggested ML model and its construction processes are described in Section 3. The performance assessment of machine learning classification algorithms using various datasets is the basis of Section 4. Furthermore described are a number of evaluation-related experiments. The outcome of this investigation and plans for further research are presented in Section 5. An attack detection system that operates via a network monitors network traffic for any unauthorised, strange, or suspicious behaviour that might indicate a cyber attack. "Acquired knowledge" is the foundation of network-based intrusion detection [9]. Both host-based and network-based intrusion detection systems are used. Intermodal technology is being used more frequently for internet-connected things such as intrusion detection systems as technology advances. The connected thing intrusion detection system now operates more effectively and efficiently. Scientific researchers' focus on intellectualization and distribution is expanding as a result of network complexity related attack diversification issues [10]. Model for a system that detects and prevents intrusions Preprocessing, categorization, and security areas make up our infrastructure detection and mitigation of intrusions system (IDPS), as demonstrated in The computer transfers the packet data after detecting the Ethernet packet. a stage of preprocessing where significant features are extracted in order to build a record of data over time. In order to identify the different forms of assaults, the data is forwarded to the classification department for pre-processing; otherwise, it is just typical network activity. The security section receives the outcome of this part next [11]. The following can be used to explain infrastructure methods for intrusion detection in light of really well datasets include UNSW-NB15 and CICIDS2017. An innovative technique for anomaly identification in an IoT setting is given utilising a bi-directional LSTM network. The UNSW-NB15 dataset was used to train and test the model, and the outcomes were remarkably good, with accuracy scores of 95.71% and f1-score values of 98.00%. The sequencing size is also left unspecified [12]. Infrastructure (NIDS) and host-based IDS consist of two types of systems for detection of intrusions (HIDS) The former uses packet interception and interrogation to raise alarms by listening in on network activity. Dedicated hosts and specialised hardware are frequently needed for NIDS. The latter based its energy on the particular action that each unique host experiences. Host-based security tools can identify recurrently unsuccessful intrusion attempts or changes to resources that are necessary for the system to function normally [13]. The displacement framework is offered as an intrusion detection approach that hierarchically incorporates an anomaly - based intrusion detection model with a model for anomaly detection. The abuse classifier is initially divided using the standard training data model. into smaller subsets after it has been built using the C4.5 decision tree technique. The deconstructed subsets are then used to generate a number of one-class SVM models. Each adversarial learning model consequently extremely correctly tracks the typical behaviour in addition to indirectly using known attack information. The NSL-KDD dataset is used to conduct experiments on the recommended hybrid intrusion detection approach. Experimental findings show that the suggested method has a lower false positive rate while outperforming traditional techniques in the sense of attack detection rates for both known and unknown threats [14]. But as Zarpelco et al. point out, systems to identify intrusions have long been researched. Three main factors have contributed to traditional IDS's inability to secure connected devices: the devices' limited resources make it impossible for them to run a classic agent; mesh networks, in which smart devices frequently operate, allow them to describes the path when they serve as the endpoint; and the wide variety of technologies and networking devices used in the IoT. HIDS have also received minimal attention, as demonstrated by Zarpelco et al. Only NIDS has studied this [15]. NIDSs, or network-based In order to recognise and protect against intrusions, intrusion detection systems a wide variety of assaults. These defences have obviously restricted capabilities, but it is unclear exactly what their advantages and disadvantages are. Flow-based and packet-based NIDS are two separate types, and the reliability of the former should be carefully evaluated using datasets with proven ground truth. In this piece, we offer the results of our empirical investigation that compared the effectiveness of flow-based and tcp is a connection NIDSs utilising a cutting-edge dataset. As a result, we are able to gain preliminary understanding in order to characterise the difference between flow-based and tcp is a connection NIDS [16]. The majority of new assaults use a known attack version, and cybersecurity relies on the similarity of these attack variants' parameters to identify them. Each dataset record has 41 network connection-derived parameters (such as duration, protocol type, service, flag, etc.), as well as a label that indicates whether the record is a normal one or one that represents a particular attack type. These characteristics can all be expressed as continuous, discrete, or composite variables [17]. The surveillance system (IDS) has grown to be a crucial component of security systems. In a world where invasive activities and security breaches are on the rise, detection of intrusions (IDS) are important security measures. Over the years, ITS system research has exploded in an effort to develop the greatest ITS system. The issue is split into detection and avoidance systems since comprehensive prevention is not attainable with current intrusion prevention systems. IDS systems use specific categorization engines to find intrusions. Web filtering systems (IPS) are then employed [18]. Network-based systems that employ misuse detection methods are the most widely used intrusion detection systems. One example of a network-based maltreatment detection system is Turbulence and ISS's Real Safeguard, which, in the open-source and business worlds, respectively, constitute the top solutions. One issue with misuse protection systems is that the calibre of their samples, frequently referred to as "signatures," has a significant impact on how well they reliably identify attacks. A flawless model is able to accurately identify every incidence of the modelling attack [19]. A cloud system can be effectively protected using an intrusion detection and mitigation system (IDPS), which has both early warning and prevention capabilities. A traditional IDS can be set up and operated as an IPS. For example, Snort can be set up in inline mode to be employed in connection with a common firewall system like Iptables to deploy IPS in a commercial networking environment. Nonetheless, such standard IPS has a number of issues: 1) Delay: In-bound IPS must examine each network packet and take preventive action, which uses up resources on the cloud system and delays detection; 2) Resource consumption: Maintaining IDPS services often uses a lot of resources [20].

2. MATERIAL AND METHOD

Network Security: By preventing various forms of possible threats from joining or spreading throughout the network, network security is a collection of technologies that safeguards the functionality and integrity of an agency's infrastructure. Network security is essential because it defends sensitive data against cyberattacks and ensures that the networking will keep working as intended. Successful online security plans employ a variety of security measures to protect users and businesses from viruses and other threats like distributed denial-of-service attacks. The term "network security" is general and refers to a number of different technologies, instruments, and practises. It can be encapsulated as a set of rules and specifications developed to protect the availability, accuracy, and confidentiality of telecommunication networks and data utilising hardware and software technologies.

Intrusion Detection System: An intruder detection system (IDS) is a monitoring tool that searches for unusual behaviour and sounds an alarm when it does. Based on these notifications, a Cybersecurity Center (SOC) detective or incident handler might look into the situation and take the required actions to eliminate the threat. This illustrative traffic restriction strategy identifies suspicious network activity, such as an unusually large number of TCP connections. This is an illustration of an IDS attacker policy that focuses on restricted IP alternatives for all ports, local IPv6 addresses, and remote IPv6 addresses.

Neural Networks: Deep learning algorithms are built around neural networks, which are also known as neural networks made up of pixels (ANNs) or simulated neural networks (SNNs). Its moniker and organizational design are derived from the human brain and correspond to how organic neurons communicate with one another. Computers can now make sound decisions with little to no human input thanks to neural networks. This is due to their capacity to learn and predict links between data input and output that are both linear and complicated. The Hopfield system, multilayer perceptron, Boltzmann machine, and Kohonen network are a few examples of various neural network types. The multi-layer perceptron will be explored in length as it is the most widely used and effective neural network.

Training Functions: The purpose of initiatives for instruction and growth is to improve an individual's or a company's efficiency at work through training activities carried out by a company organization. These programmers frequently involve improving a worker's incentive to perform better on the job while also enhancing their knowledge and skill sets. A training activity called management training focuses on improving a person's capacity for management and leadership. Soft skills like empathy and communication, which foster better teamwork and closer relationships with the individuals they manage, may be increased in importance weight.

Method: SPSS Statistics is a statistical control Advanced Analytics, Multivariate Analytics, Business enterprise Intelligence and IBM a statistic created by a software program is a package crook research. A set of generated statistics is Crook Research is for a long time SPSS Inc. Produced by, it was acquired by IBM in 2009. Current versions (after 2015) icon Named: IBM SPSS Statistics. The name of the software program is to start with social Became the Statistical Package for Science (SPSS) [3] Reflects the real marketplace, then information SPSS is converted into product and service solutions Widely used for statistical evaluation within the social sciences is an application used. pasted into a syntax statement. Programs are interactive Directed or unsupervised production Through the workflow facility. SPSS Statistics is an internal log Organization, types of information, information processing and on applicable documents imposes regulations, these jointly programming make it easier. SPSS datasets are two-dimensional Have a tabular structure, in which Queues usually form Events (with individuals or families) and Columns (age, gender or family income with) to form measurements. of records Only categories are described: Miscellaneous and Text content (or "string"). All statistics Processing is also sequential through the statement (dataset) going on Files are one-to-one and one-to-one Many can be matched, although many are not in addition to those case-variables form and by processing, there may be a separate matrix session, There you have matrix and linear algebra on matrices using functions Information may be processed.

3. RESULTS AND DISCUSSION

TABLE 1. Descriptive Statistics

	N	Range	Minimum	Maximum	Mean		Std. Deviation	Variance
Network Security	150	4	1	5	3.81	.100	1.228	1.509
Intrusion Detection System	150	4	1	5	4.17	.064	.789	.623
Neural Networks	150	4	1	5	4.08	.086	1.059	1.121
Training Functions	150	4	1	5	4.26	.063	.772	.596
Valid N (listwise)	150							

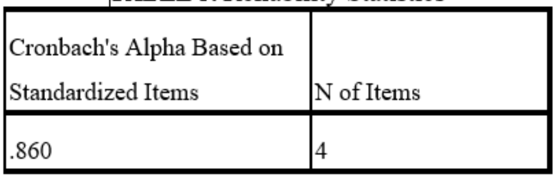
Table 1 shows the descriptive statistics values for analysis N, range, minimum, maximum, mean, standard deviation Network Security, Intrusion Detection System, Neural Networks and Training Functions this also using.

TABLE 2. Frequencies Statistics

		Network Security	**Intrusion Detection System**	**Neural Networks**	**Training Functions**
N	Valid	150	150	150	150
	Missing	0	0	0	0
Mean		3.81	4.17	4.08	4.26
Std. Error of Mean		.100	.064	.086	.063
Median		4.00	4.00	4.00	4.00
Mode		4	4	4	4
Std. Deviation		1.228	.789	1.059	.772
Variance		1.509	.623	1.121	.596
Skewness		-1.025	-2.298	-1.949	-2.259
Std. Error of Skewness		.198	.198	.198	.198
Kurtosis		-.082	8.173	3.646	8.359
Std. Error of Kurtosis		.394	.394	.394	.394
Range		4	4	4	4
Minimum		1	1	1	1
Maximum		5	5	5	5
Sum		572	625	612	639
Percentiles	25	4.00	4.00	4.00	4.00
	50	4.00	4.00	4.00	4.00
	75	5.00	5.00	5.00	5.00

Table 2 Show the Frequency Statistics in Network based Intrusion Detection System Network Security, Intrusion Detection System, Neural Networks and Training Functions curve values are given.

TABLE 3. Reliability Statistics



Cronbach's Alpha Based on Standardized Items	N of Items
.860	4

Table 3 shows The Cronbach's Alpha Reliability result. The overall Cronbach's Alpha value for the model is .860 which indicates 86% reliability. From the literature review, the above 50% Cronbach's Alpha value model can be considered for analysis.

TABLE 4. Reliability Statistic individual

	Cronbach's Alpha if Item Deleted
Network Security	.418
Intrusion Detection System	.376
Neural Networks	.394
Training Functions	.396

Table 4 Shows the Reliability Statistic individual parameter Cronbach's Alpha Reliability results. The Cronbach's Alpha value for Network Security .418, Intrusion Detection System .376, Neural Networks .394 and Training Functions .396 this indicates all the parameters can be considered for analysis.

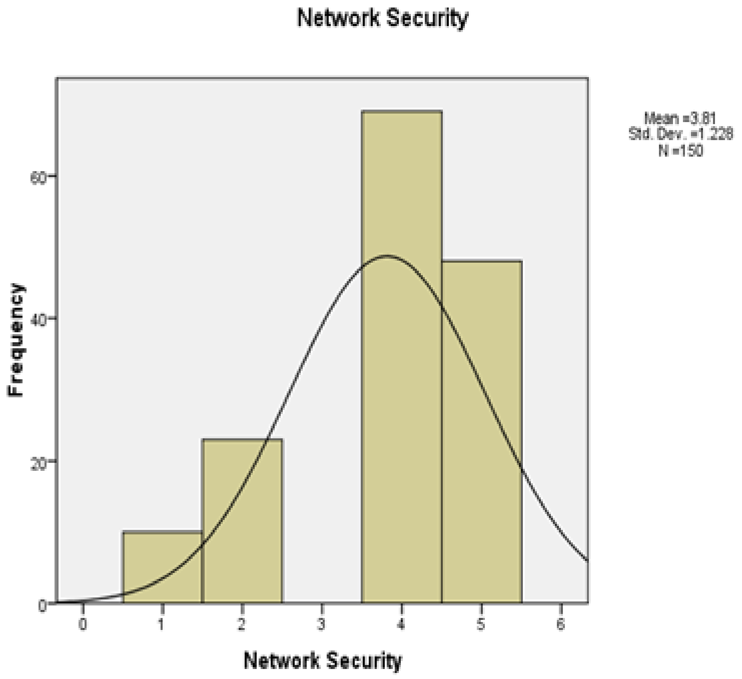


FIGURE 1. Network Security

Figure 1 shows the histogram plot for Network Security from the figure it is clearly seen that the data are slightly right skewed due to more respondent chosen 4 for Network Security except the 2 value all other values are under the normal curve shows model is significantly following normal distribution.

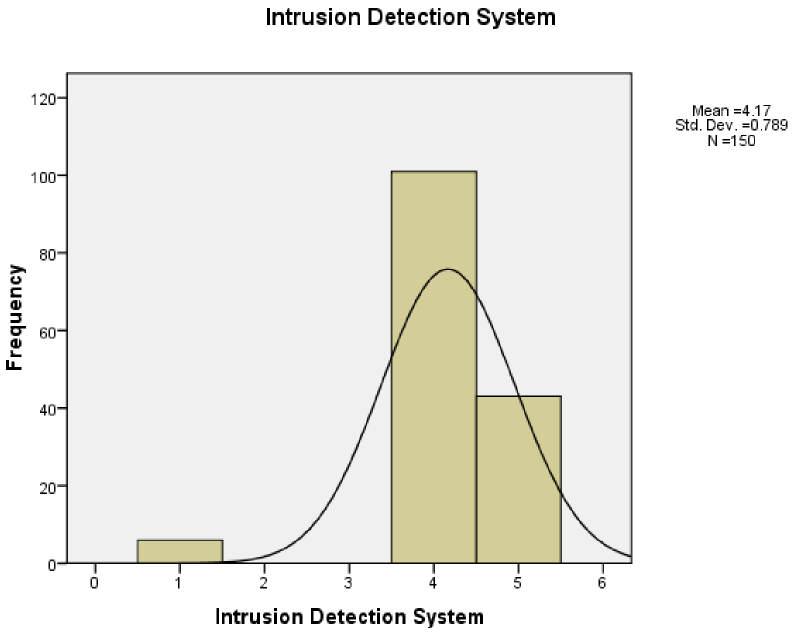


FIGURE 2. Intrusion Detection

Figure 2 shows the histogram plot for Intrusion Detection from the figure it is clearly seen that the data are slightly Left skewed due to more respondent chosen 4 for Intrusion Detection except the 2 value all other values are under the normal curve shows model is significantly following normal distribution.

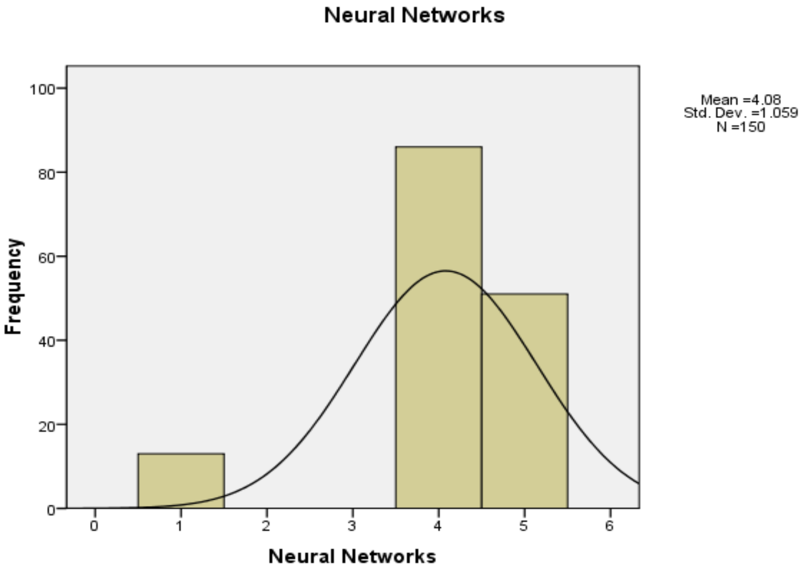


FIGURE 3. Neural Networks

Figure 3 shows the histogram plot for Neural Networks from the figure it is clearly seen that the data are slightly Left skewed due to more respondent chosen 4 for Neural Networks except the 2 value all other values are under the normal curve shows model is significantly following normal distribution.

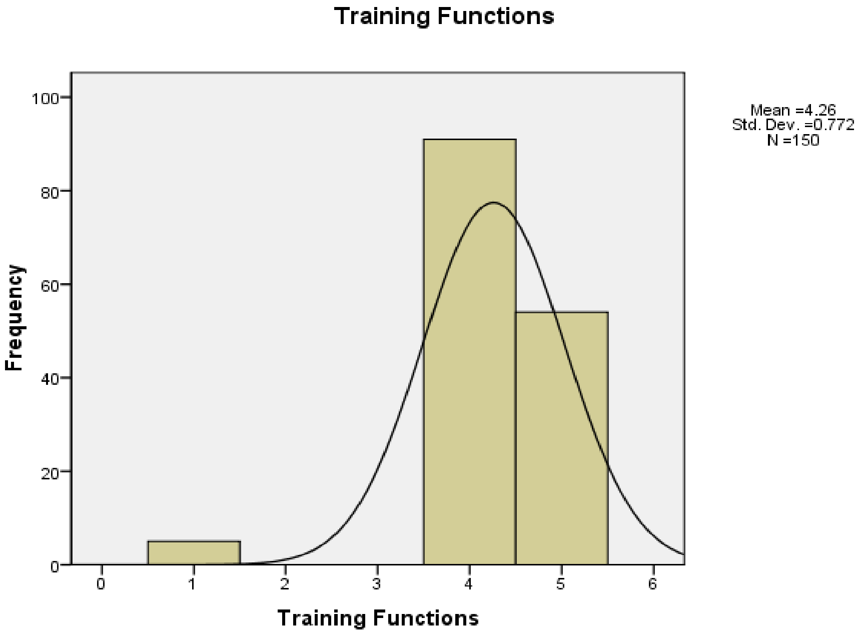


FIGURE 4. Training Functions

Figure 4 shows the histogram plot for Training Functions from the figure it is clearly seen that the data are slightly Left skewed due to more respondent chosen 4 for Training Functions except the 2 value all other values are under the normal curve shows model is significantly following normal distribution.

TABLE 5. Correlations

	Network Security	**Intrusion Detection System**	**Neural Networks**	**Training Functions**
Network Security	1	.219**	.203*	.108
Intrusion Detection System	.219**	1	.128	.281**
Neural Networks	.203*	.128	1	.212**
Training Functions	.108	.281**	.212**	1
**. Correlation is significant at the 0.01 level (2-tailed) *. Correlation is significant at the 0.05 level (2-tailed)				

Table 5 shows the correlation between motivation parameters for Network Security. For Intrusion Detection System is having highest correlation with Training Functions and having lowest correlation. Next the correlation between motivation parameters for Intrusion Detection System. For Training Functions is having highest correlation with Neural Networks and having lowest correlation. Next the correlation between motivation parameters for Neural Networks. For Training Functions is having highest correlation with Intrusion Detection System and having lowest correlation. Next the correlation between motivation parameters for Training Functions. For Intrusion Detection System is having highest correlation with Network Security and having lowest correlation.

4. CONCLUSION

An invasion detection system (NIDS) that makes use of networks can spot malicious activities on a network. For NIDS to inspect each and every packet of communication, including unicast traffic, invalid network access is often required. Along with being small structures that don't block traffic, NIDS are able to keep an eye on usernames and passwords, check for any signs of odd activity in the file integrity logs, port logs, mysql database file storage, etc. and alert the part of implementing as necessary. In the past decades, due to developments Increased use of networking techniques and internet, digital Contacts entered into everything that happens on the world market. The hacker penetration attempts are taking place in parallel with these advances. Networks are expanding as well. Without permission, they attempted to modify some network data or increase network traffic in order to launch a denial-of-service attack. Intrusion prevention systems (IDS) are also favored. Intrusion detection is the process of spotting intruders' attacks on information systems. These actions, which are sometimes known as incursions, are meant to obtain unrestricted control over a computer system. External or internal intruders both exist. Those who have a modicum of valid access to the network but try to abuse unauthorized powers by elevating their access privileges are known as internal invaders. Users just outside of the target network are considered external intruders when they attempt to access system data without authorization. By preventing various forms of possible threats from joining or spreading throughout the network, network security is a collection of technologies that safeguards the functionality and integrity of an agency's infrastructure. Deep learning algorithms are built around neural networks, which are also known as neural networks made up of pixels (ANNs) or simulated neural networks (SNNs). Its moniker and organizational design are derived from the human brain and correspond to how organic neurons communicate with one another. Computers can now make sound decisions with little to no human input thanks to neural networks. The purpose of initiatives for instruction and growth is to improve an individual's or a company's efficiency at work through training activities carried out by a company organization. These programmers frequently involve improving a worker's incentive to perform better on the job while also enhancing their knowledge and skill sets. SPSS statistics is a multivariate analytics, business intelligence, and criminal investigation data management, advanced analytics, developed by IBM for a statistical software package. A long time, spa inc. Was created by, IBM purchased it in 2009. The brand name for the most recent versions is IBM SPSS statistics. Network Security, Intrusion Detection System, Neural Networks and Training Functions. The Cronbach's Alpha Reliability result. The overall Cronbach's Alpha value for the model is .860which indicates 86% reliability. From the literature review, the above 50% Cronbach's Alpha value model can be considered for analysis.

REFERENCES

[1]. Zarpelão, Bruno Bogaz, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, and Sean Carlisto de Alvarenga. "A survey of intrusion detection in Internet of Things." *Journal of Network and Computer Applications* 84 (2017): 25-37.

[2]. Karatas, Gozde, and Ozgur Koray Sahingoz. "Neural network based intrusion detection systems with different training functions." In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pp. 1-6. IEEE, 2018.

[3]. Ring, Markus, Sarah Wunderlich, Deniz Scheuring, Dieter Landes, and Andreas Hotho. "A survey of network-based intrusion detection data sets." Computers & Security 86 (2019): 147-167.

[4]. Prasanalakshmi, B., and A. Farouk. "Classification and prediction of student academic performance in king khalid university-a machine learning approach." Indian J Sci Technol 12 (2019): 14.

[5]. Bumb, Swapnil Sunil, Dara John Bhaskar, Chandan R. Agali, Himanshu Punia, Vipul Gupta, Vikas Singh, Safalya Kadtane, and Sneha Chandra. "Assessment of photodynamic therapy (PDT) in disinfection of deeper dentinal tubules in a root canal system: an in vitro study." Journal of clinical and diagnostic research: JCDR 8, no. 11 (2014): ZC67.

[6]. Patel BJ, Surana P, Patel KJ. Recent Advances in Local Anesthesia: A Review of Literature. Cureus. 2023 Mar 17;15(3):e36291. doi: 10.7759/cureus.36291. PMID: 37065303; PMCID: PMC10103831.

[7]. Vigna, Giovanni, and Richard A. Kemmerer. "NetSTAT: A network-based intrusion detection system." Journal of computer security 7, no. 1 (1999): 37-71.

[8]. Vimala Saravanan, Babila revathy M, M Ramachandran, Ashwini Murugan, "Understanding Indian Technical Institution using TOPSIS MCDM Method", REST Journal on Data Analytics and Artificial Intelligence , 1(1), (2022):23-29

[9]. Ahuja, Sakshi, Vidya Dodwad, Bhavna Jha Kukreja, Praful Mehra, and Pankaj Kukreja. "A comparative evaluation of efficacy of Punica granatum and chlorhexidine on plaque and gingivitis." Journal of the International Clinical Dental Research Organization 3, no. 1 (2011): 29-32.

[10]. Linda, Ondrej, Todd Vollmer, and Milos Manic. "Neural network based intrusion detection system for critical infrastructures." In 2009 international joint conference on neural networks, pp. 1827-1834. IEEE, 2009.

[11]. Asharf, Javed, Nour Moustafa, Hasnat Khurshid, Essam Debie, Waqas Haider, and Abdul Wahab. "A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions." Electronics 9, no. 7 (2020): 1177.

[12]. Krishna, S. Rama, Ketan Rathor, Jarabala Ranga, Anita Soni, D. Srinivas, and Anil Kumar. "Artificial Intelligence Integrated with Big Data Analytics for Enhanced Marketing." In 2023 International Conference on Inventive Computation Technologies (ICICT), pp. 1073-1077. IEEE, 2023.

[13]. Kadtane, Safalya S., D. J. Bhaskar, Chandan Agali, Himanshu Punia, Vipul Gupta, Manu Batra, Vikas Singh, and Swapnil S. Bumb. "Periodontal health status of different socio-economic groups in out-patient department of TMDC & RC, Moradabad, India." Journal of clinical and diagnostic research: JCDR 8, no. 7 (2014): ZC61.

[14]. Kim, Dong Seong, and Jong Sou Park. "Network-based intrusion detection with support vector machines." In Information Networking: International Conference, ICOIN 2003, Cheju Island, Korea, February 12-14, 2003. Revised Selected Papers, pp. 747-756. Springer Berlin Heidelberg, 2003.

[15]. Jomon Jos, Vidhya Prasanth, M. Ramachandran, Ashwini Murugan, "Analysis of Blind Spot in Heavy Vehicles Driving Using VIKOR Method", REST Journal on Data Analytics and Artificial Intelligence , 1(1), (2022):15-22

[16]. Prasanalakshmi, B., and A. Kannammal. "Secure credential federation for hybrid cloud environment with SAML enabled multifactor authentication using biometrics." International Journal of Computer Applications 53, no. 18 (2012).

[17]. Kukreja, Bhavna Jha, Kishore Gajanan Bhat, Pankaj Kukreja, Vijay Mahadev Kumber, Rajkumar Balakrishnan, and Vivek Govila. "Isolation and immunohistochemical characterization of periodontal ligament stem cells: A preliminary study." Journal of Indian Society of Periodontology 25, no. 4 (2021): 295.

[18]. Ferrag, Mohamed Amine, Leandros Maglaras, Ahmed Ahmim, Makhlouf Derdour, and Helge Janicke. "Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks." Future internet 12, no. 3 (2020): 44.

[19]. Bagde, Hiroj, Savitha Banakar, Alka Waghmare, Ashwini Bagde, Shailendra Singh Chaturvedi, and Santosh Rayagouda Patil. "Assessment of the Relationship Between Matrix Metalloproteinase-9 Promoter Gene Polymorphism and Chronic Periodontitis." Pesquisa Brasileira em Odontopediatria e Clínica Integrada 21 (2021).

[20]. Kumar, Sanjay, Ari Viinikainen, and Timo Hamalainen. "Machine learning classification model for network based intrusion detection system." In 2016 11th international conference for internet technology and secured transactions (ICITST), pp. 242-249. IEEE, 2016.

[21]. Chinnasami Sivaji, P.K.Chidambaram, M. Ramachandran, Ashwini Murugan, "Performance Analysis of Facade Materials using VIKOR Method", REST Journal on Advances in Mechanical Engineering, 1(2), (2022):41-49.

[22]. Rathor, Ketan, Anshul Mandawat, Kartik A. Pandya, Bhanu Teja, Falak Khan, and Zoheib Tufail Khan. "Management of Shipment Content using Novel Practices of Supply Chain Management and Big Data Analytics." In 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), pp. 884-887. IEEE, 2022.

[23]. Bhargava, Deepshikha, B. Prasanalakshmi, Thavavel Vaiyapuri, Hemaid Alsulami, Suhail H. Serbaya, and Abdul Wahab Rahmani. "CUCKOO-ANN based novel energy-efficient optimization technique for IoT sensor node modelling." Wireless Communications and Mobile Computing 2022 (2022): 1-9.

[24]. Kim, Soung Min, Suk Keun Lee, Sam Paul, Rupshikha Choudhury, Nandini Kumari, Sanjay Rastogi, Ashish Sharma, Vikas Singh, Shyamalendu Laskar, and Tushar Dubey. "Is treatment with platelet-rich fibrin better than zinc oxide eugenol in cases of established dry socket for controlling pain, reducing inflammation, and improving wound healing?." Journal of the Korean Association of Oral and Maxillofacial Surgeons 45, no. 2 (2019): 76-82.

[25]. Bawa, Surjit Singh. "Implementing Text Analytics with Enterprise Resource Planning."

[26]. Yang, Aimin, Yunxi Zhuansun, Chenshuai Liu, Jie Li, and Chunying Zhang. "Design of intrusion detection system for internet of things based on improved BP neural network." Ieee Access 7 (2019): 106043-106052.

[27]. Kukreja, Bhavna Jha, Udayan Gupta, Vidya Dodwad, and Pankaj Kukreja. "Periosteal fenestration vestibuloplasty procedure for sulcus deepening in a hemimandibulectomy patient following implant therapy." Journal of Indian Society of Periodontology 18, no. 4 (2014): 508.

[28]. Singh, Vikas, D. J. Bhaskar, R. Chandan Agali, Varunjeet Chaudhary, Swapnil S. Bumb, and Chaitanya Dev Jain. "Knowledge and attitude towards droplet and airborne isolation precautions and its correlation among students of TMDC&RC, Moradabad." Int J Adv Health Sci 1, no. 3 (2014): 8-15.

[29]. Manjunath, C. R., Ketan Rathor, Nandini Kulkarni, Prashant Pandurang Patil, Manoj S. Patil, and Jasdeep Singh. "Cloud Based DDOS Attack Detection Using Machine Learning Architectures: Understanding the Potential for Scientific Applications." International Journal of Intelligent Systems and Applications in Engineering 10, no. 2s (2022): 268-271.

[30]. Duraisamy, Sathya, Ganesh Kumar Pugalendhi, and Prasanalakshmi Balaji. "Reducing energy consumption of wireless sensor networks using rules and extreme learning machine algorithm." The Journal of Engineering 2019, no. 9 (2019): 5443-5448.

[31]. Wattanapongsakorn, Naruemon, S. Srakaew, E. Wonghirunsombat, C. Sribavonmongkol, T. Junhom, P. Jongsubsook, and Chalermpol Charnsripinyo. "A practical network-based intrusion detection and prevention system." In 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 209-214. IEEE, 2012.

[32]. Oliveira, Nuno, Isabel Praça, Eva Maia, and Orlando Sousa. "Intelligent cyber attack detection and classification for network-based intrusion detection systems." Applied Sciences 11, no. 4 (2021): 1674.

[33]. Bawa, Surjit Singh. "How Business can use ERP and AI to become Intelligent Enterprise."

[34]. Amaral, João P., Luís M. Oliveira, Joel JPC Rodrigues, Guangjie Han, and Lei Shu. "Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks." In 2014 IEEE international conference on communications (ICC), pp. 1796-1801. IEEE, 2014.

[35]. Asmita Mahajan, M. Ramachandran, Sathiyaraj Chinnasamy, Ashwini Murugan, "Evaluating sustainable transportation systems using Weight Product method", REST Journal on Advances in Mechanical Engineering, 1(2),(2022): 33-40

[36]. Prasanalakshmi, B., K. Murugan, Karthik Srinivasan, S. Shridevi, Shermin Shamsudheen, and Yu-Chen Hu. "Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography." The Journal of Supercomputing 78, no. 1 (2022): 361-378.

[37]. Kumar, Mukesh, Manish Goyal, Jha Bhavna, Sumit Tomar, and Ashish Kushwah. "An Innovative Procedure for Lip Lengthening in a Patient with a Short Upper Lip and High-Angle Skeletal Class II Pattern: A Case Report." Journal of Indian Orthodontic Society 55, no. 3 (2021): 315-322.

[38]. Kumar, Ashish, Ketan Rathor, Snehit Vaddi, Devanshi Patel, Preethi Vanjarapu, and Manichandra Maddi. "ECG Based Early Heart Attack Prediction Using Neural Networks." In 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), pp. 1080-1083. IEEE, 2022.

[39]. Chopra, Amandeep, Manav Lakhanpal, Vikas Singh, Nidhi Gupta, N. C. Rao, and Varun Suri. "The habit of digit sucking among children and the attitude of mothers towards the habit in India." TMU J Dent 2, no. 1 (2015): 1-4.

[40]. Mazini, Mehrnaz, Babak Shirazi, and Iraj Mahdavi. "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms." Journal of King Saud University-Computer and Information Sciences 31, no. 4 (2019): 541-553.

[41]. Prasanalakshmi, B., A. Kannammal, and R. Sridevi. "Frequency domain combination for preserving data in space specified token with high security." In Informatics Engineering and Information Science: International Conference, ICIEIS 2011, Kuala Lumpur, Malaysia, November 12-14, 2011. Proceedings, Part I, pp. 319-330. Springer Berlin Heidelberg, 2011.

[42]. Gassais, Robin, Naser Ezzati-Jivan, Jose M. Fernandez, Daniel Aloise, and Michel R. Dagenais. "Multi-level host-based intrusion detection system for Internet of things." Journal of Cloud Computing 9 (2020): 1-16.

[43]. Ficke, Eric, Kristin M. Schweitzer, Raymond M. Bateman, and Shouhuai Xu. "Characterizing the effectiveness of network-based intrusion detection systems." In MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM), pp. 76-81. IEEE, 2018.

[44]. Dias, Leonardo P., Jés de Jesus Fiais Cerqueira, Karcius DR Assis, and Raul C. Almeida. "Using artificial neural network in intrusion detection systems to computer networks." In 2017 9th Computer Science and Electronic Engineering (CEEC), pp. 145-150. IEEE, 2017.

[45]. Nayeemuddin, M. Ramachandran, Chinnasami Sivaji, Prabakaran Nanjundan, "A Study on Renewable Energy and Wind Power", REST Journal on Advances in Mechanical Engineering, 1(2), (2022):10-18.

[46]. Rathor, Ketan, Keyur Patil, Mandiga Sahasra Sai Tarun, Shashwat Nikam, Devanshi Patel, and Sasanapuri Ranjit. "A Novel and Efficient Method to Detect the Face Coverings to Ensurethe Safety using Comparison Analysis." In 2022 International Conference on Edge Computing and Applications (ICECAA), pp. 1664-1667. IEEE, 2022.

[47]. Chaudhury, Sushovan, Nilesh Shelke, Kartik Sau, B. Prasanalakshmi, and Mohammad Shabaz. "A novel approach to classifying breast cancer histopathology biopsy images using bilateral knowledge distillation and label smoothing regularization." Computational and Mathematical Methods in Medicine 2021 (2021): 1-11.

[48]. Bawa, Surjit Singh. "Implement Gamification to Improve Enterprise Performance." International Journal of Intelligent Systems and Applications in Engineering 11, no. 2 (2023): 784-788.

[49]. Bumb, Swapnil S., D. J. Bhasker, Chandan R. Agali, Himanshu Punia, Vikas Singh, and Safalya Kadtane. "Comparison of oral health knowledge, attitudes, practices and oral hygiene status of Central Reserve Police Force officials in Srinagar, Kashmir." Elective Medicine Journal 2, no. 1 (2014): 10-14.

[50]. Kukreja, Pankaj, Modi Fahd Al Qahtani, Majedah Fahd Al Qahtani, Ahad Fahd Al Qahtani, and Bhavna Jha Kukreja. "Use of stem cells in tissue engineering and reconstruction of the maxillofacial region." International Journal of Research in Medical Sciences 8, no. 7 (2020): 2740.

[51]. Sathiyaraj Chinnasamy, P.K.Chidambaram, M. Ramachandran, Malarvizhi Mani, “Performance Analysis of Sustainable Production Using VIKOR Method”, REST Journal on Advances in Mechanical Engineering, 1(1), (2022):32-39.

[52]. Nayyar, Sanchit, Sneha Arora, and Maninder Singh. "Recurrent neural network based intrusion detection system." In 2020 international conference on communication and signal processing (iccsp), pp. 0136-0140. IEEE, 2020.

[53]. Vigna, Giovanni, William Robertson, and Davide Balzarotti. "Testing network-based intrusion detection signatures using mutant exploits." In Proceedings of the 11th ACM conference on Computer and communications security, pp. 21-30. 2004.

[54]. Rathor, Ketan, Sushant Lenka, Kartik A. Pandya, B. S. Gokulakrishna, Susheel Sriram Ananthan, and Zoheib Tufail Khan. "A Detailed View on industrial Safety and Health Analytics using Machine Learning Hybrid Ensemble Techniques." In 2022 International Conference on Edge Computing and Applications (ICECAA), pp. 1166-1169. IEEE, 2022.

[55]. Sujith, A. V. L. N., Guna Sekhar Sajja, V. Mahalakshmi, Shibili Nuhmani, and B. Prasanalakshmi. "Systematic review of smart health monitoring using deep learning and Artificial intelligence." Neuroscience Informatics 2, no. 3 (2022): 100028.

[56]. Xing, Tianyi, Zhengyang Xiong, Dijiang Huang, and Deep Medhi. "SDNIPS: Enabling software-defined networking based intrusion prevention system in clouds." In 10th International Conference on Network and Service Management (CNSM) and Workshop, pp. 308-311. IEEE, 2014.