International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020

Novel Trust Based Ranking for Intrusion Detection and Security using Deep Learning

J. Josemila Baby, J. R. Jeba

Abstract: ***Network intrusions are turning out to be increasingly more complex to distinguish. To moderate this subject, intrusion detection systems (IDSs) have been broadly deploying in distinguishing an assortment assaults. A lot of consideration has been given to profound learning during recent days, and latest profound knowledge procedures be developing by superior functionality. Numerous PC with system application effectively use such profound learn calculations and report upgraded execution throughout them. In this article, we plan and assess an IDS utilizing profound learning and trust the executive's component that enables gadgets to manage disrepute data about their neighbors. The proposed IDS method at first plays out of a positioning procedure and specifically groups the hub utilizing profound learning system. Results and correlation on execution investigation demonstrates the predominance of the proposed IDS.***

Keywords: ***Intrusion Detection Systems (IDSs); Deep Learning; Security; Ranking process; Trust organization.***

I. INTRODUCTION

The quick expansion of computer innovation has brought about the exchange of an ever-increasing number of administrations to the computer-based systems. The reliance of a few administrations on computer innovation has brought about the expansion of computer-related threats [1]. As time passes, the shirking and detection of threats to the computer innovation is turning out to be progressively trouble [2]. The expansion in the number and seriousness of dangers has brought forth another field of study.

Network-Based computer systems assume crucial jobs in modern society; they have become the objectives of our adversary and crooks [3]. Accordingly, we have to locate the most ideal ways that are available to ensure our systems. Intrusion detection systems have risen in the computer security territory as a result of the trouble of guarantee that a data frame work will be liberated from security blemishes. Intrusion Detection System (IDS) is a product of hardware division that mechanizes the intrusion detection process [4]. It is intended to screen the occasion's event in a computer framework and system and reacts to occasions with indication of the potential episode of infraction of protection preparations [5].

The security of a computer framework is damaged when an intrusion happens. An intrusion can be characterize as "any arrangement of activities that attempt to bargain the honesty, classification or accessibility of an asset" [6]. Intrusion expectation methods, for example, client authentication (for example utilizing passwords or biometrics), abstaining from programming mistakes, and data security (e.g., encryption) have been utilized to ensure computer systems as a first line of barrier [7]. Basically, there are two fundamental kinds of intrusion detection systems: Signature-based (SBS) and anomaly-based (ABS). SBS systems depend on design acknowledgment strategies where they keep up the database of signatures of recently known assaults and contrast them and dissected information. An alert is raised when the signatures are coordinated [8]. Then again ABS systems assemble a factual model portraying the ordinary network traffic, and any unusual conduct that veers off from the model is recognized [9]. As opposed to signature-based systems, anomaly-based systems have a bit of advantage that they can recognize zero-day assaults. Though ABS (in contrast to SBS) requires a preparation stage to build up the database of general assaults and a cautious setting of a threshold level of detection makes it complex [10].

IDSs are additionally named network-based or host-based as far as wellspring of information. The previous group basic network parcels as the information source from the network and dissect for indications of intrusions Host-based IDS [11] works on data gather from inside an individual computer framework, for example, working framework review trails, C2 review logs, and System logs. Most of the IDS settled in today are either rule-based or expert-system based [12]. Their qualities rely to a great extent upon the capacity of the security staff that creates them. The previous can just recognize realized assault types and the last is inclined to the age of bogus positive alerts [13]. Thus, the requirement for insight systems known as AI methods which naturally gain from the information or concentrate a helpful example from information as a source of perspective for typical/assault traffic conduct profile from existing information for consequent arrangement of network traffic [14].

This paper is sorted out as follows. Segment II shows a portion of the difficulties of utilizing IDS for abnormality detection in networks. In Section III, we diagram the proposed design and the profound learning-based systems that we propose to use for oddity detection. Section IV shows the examinations led to exhibit the achievability of our proposition, while ends are drawn and future work is laid out in Section V.

Revised Manuscript Received on February 05, 2020.
* Correspondence Author
Josemila Baby*, Department of Computer Applications, Noorul Islam Centre for Higher Education, Kumaracoil, India.
Email: josemilababy.phd@gmail.com
J.R. Jeba, Associate Professor & Head, Department of Computer Applications, Noorul Islam Centre for Higher Education Kumaracoil, India.
Email: jebaj.phd@gmail.com

II. RELATED WORK

Krishnan, Deepa, and Madhumita Chatterjee (2012) [15] proposed a one of a kind Distributed Intrusion Detection System (DIDS) based on a novel mix of two variation slant in intrusion detection. The conduct based methodology encourages improved detection in the dynamic cloud condition and the information-based methodology underpins the detection plot with its reliable guideline base. The usefulness of both these methodologies has been improved by the expansion of a versatile methodology which serves to fundamentally help with bringing down the bogus positives. Notwithstanding that, another novel and the striking preferred position of the proposed detection plot was the alarm grouping and investigating facility in this way helping all participating hubs in identifying bogus cautions from any malignant hubs. DOS assaults in a single hub can be sent as alarms to help other participating hubs in refreshing themselves about new assault designs prompting early detection and avoidance of assaults. That plan, on the whole, makes the hidden cloud foundation increasingly safe to assaults and keeps on giving administrations to clients.

M. Ali et al., (2009) [16] proposed a crossbreed IDS by joining the two methodologies in a solitary framework. The half and half IDS was acquired by consolidating packet header abnormality recognition (PHAD) and network traffic anomaly detection (NETAD) which are anomaly-based IDSs with the abuse based IDS Snort which was an open-source venture. The half and half IDS got were assessed utilizing the MIT Lincoln Laboratories network traffic information (IDEVAL) as a test bed. The assessment thinks about the number of assaults distinguished through abuse based IDS all alone, with the crossbreed IDS got joining anomaly-based and abuse based IDSs and shows that the crossbreed IDS was a additional dominant system.

Alert correlation [17] was a procedure that breaks down the alarms created by at least one intrusion detection system and gives a progressively compact and significant level perspective on happening or endeavored intrusions. Even though the connection procedure was regularly exhibited as a solitary advance, the investigation was really completed by various parts, every one of which has an objective. Unfortunately, most ways to deal with connection focus on only a couple of parts of the procedure, giving formalisms and systems that address just explicit relationship issues. Valeur, Fredrik et al., (2004) introduced a general relationship model that incorporates a complete arrangement of segments and a system based on that model. A device utilizing the system has been applied to various surely understood intrusion detection informational collections to distinguish how every segment adds to the general objectives of connection.

Jaisankar, N et al., (2012) [18] proposed another wise specialist based IDS utilizing Fuzzy Rough Set based exception detection and Fuzzy Rough set based SVM. In that proposed model they presented two distinctive canny operators to be specific element determination specialist to choose the necessary list of capabilities utilizing fuzzy unpleasant sets and basic leadership operator director for settling on an official conclusion. Also, they have presented a fuzzy unpleasant set based anomaly detection calculation to recognize anomalies. They have additionally received Fuzzy Rough based SVM in our system to characterize and distinguish inconsistencies proficiently.

Depren, Ozgur et al., (2005) [19] proposed a novel Intrusion Detection System (IDS) design using both abnormality and abuse finding approach. That hybrid Intrusion Detection System design comprises of an abnormality detection module, an abuse the finding element and a choice of emotionally helpful to the system consolidates the after-effects of these two detection modules. The proposed abnormality recognition module uses a Self-Organizing Map (SOM) structure to exhibit customary direct. Deviation from the customary lead was named an attack. The proposed misuse discovery module uses J.48 decision tree computation to aggregate various types of attacks. The rule eagerness of that work was to benchmark the show of the proposed half and half IDS design.

III. PROPOSED TECHNIQUE

Intrusion detection innovation is another security bolster component and screens the network system without influencing the network execution to prevent internal and external assaults and abuse. Intrusion detection systems have an assortment of groupings. In this segment, we plan and assess a few IDS components for the Internet of Things Networks that is fit to little gadgets. They utilize a trust the executive's system that enables gadgets to oversee notoriety data about their neighbors.

A. Trust Evaluation

This segment is answerable for assessing the reliability of different hubs. In this work, weprimarily consider two sorts of trust:

- Feedback based trust
- Packet-based trust

Aiming to provide a comprehensive trust evaluation in this component:

- Feedback-based trust is set up based on the feedback from partner nodes (which show up in the accomplish list). The feedback will be sent and got by a coordinated effort section.
- Packet-based trust is figured depends on the got amiable packets and complete packets from the objective hub. These kinds of trust are objective and are useful for deciding a trusted route and identify intending nodes.

a. Packet based Trust Evaluation

More specially, the replies from a node i are ordered from the most recent to the oldest according to the time t_k at which they have been received by node$j$. The trust worthiness of node i according to node j can then be estimated as follows:

$$T_i^j(Packet) = \left[\left(\sum_{k=0}^{n} S_k^{j,i} F^{t_k}\right)(F^{t_k})^{-1}\right] \quad (1)$$

Where $S_k^{j,i} \in [0,1]$the satisfaction of the respond k and n is is the total amount of feedback. Table 1 shows the satisfaction value it will assign once a node receives the feedback. Based on the satisfactory level of its feedback the trust values of every node will be updated.

Table1: Satisfaction Values

Satisfaction Values	Condition
1.0	Very satisfied
0.5	Satisfied
0.3	Neutral
0.1	Not satisfied
0	Not satisfied

Above table1 speaks to the states of agreeable qualities. To manage potential changes of the hub, conduct after some time, we utilize an overlooking component $F(0 \leq F \leq 1)$which helps in doling take away load to more established feedback reactions.

b. Feedback based Trust Evaluation

The assessment of the dependability of a hub is completed utilizing test messages conveyed occasionally utilizing an irregular toxic substance process. So as to urge hubs to give acceptable feedback reactions at whatever point conceivable, the trust worth will be gradually refreshed each time the hub gives a "don't have the foggiest idea" reply. The honesty of a node i
according to node j is then formulated as follows:

$$T_i^j(Feedback) = \left(T_i^j(Packet) - T_{stranger}\right)(1-x)^m + T_{stranger} \quad (2)$$

Here$x$ is the percentage of unknown answer from time 0 to 10, the positive enticement parameter (forgetting responsibility) is to control the harshness of penalty to “don’t know” response ,$T_i^j(Packet)$is the trust value without the addition of “don’t know” answers equation (1), and $T_{stranger}$ is the defaulting trust value of a unfamiliar person. In the end, the trust worth will turn into that of an outsider. This permits the belief estimation of an entrust hub to gradually increment up to the degree of an outsider by giving "don't have a clue" answers. Moreover, hubs with little experience are roused to give "don't have the foggiest idea" answers as opposed to erroneous alert ranking.

Depending on overall trustworthiness, each node i requests alert by consulting the other nodes from its known list which explains that trust values better than the threshold $thre_t^i$. Feedback from the neighboring an acquaintances is more applicable than that distant ones. We measure the proximity related to the region in which the node belongs to. Once the feedback is received from the acquaintance list, node j collects the feedback by using ahighly weighted method as follows:

$$A_j(R) = \sum_{T_i^j \geq thre_i^j} \left[\left(T_i^j(Packet) D_i^j A_i(R)\right)_{\left(T_i^j(Feedback) D_i^j\right)}\right]^{-1} \quad (3)$$

A_j(R)is the aggregated ranking of alert. Given feedback is by each node that belongs to the acquaintance list of node.T_i^j (∈[0, 1]) is the trust value of nodes according to node j. D_i^j(∈[0,1]) is the accessibility weight of nodes.⟦thre⟧$e_t^i$is the trust threshold set by node j. $A_i(R)$(∈[0,1]) is the feedback ranking of alerts by nodes.

c. Total Trust Evaluation

The total trust worth will be determined utilizing the aggregate of packet based trust assessment just as feedback based trust assessment. Utilizing the condition 4 shows we will locate the complete trust assessment,

$$T_i^j(Total) = T_i^j(Packet) + T_i^j(Feedback) \quad (4)$$

Table 2 speaks to the trust esteems based positioning. Utilizing the trust esteems we rank it and order the intrusion.

Table2: Trust values based ranking and classification

Trust Value	Rank	Classification
0.9-1.0	1	Non-Intruded
<0.9	2	Maybe intruded

If the rank is 1 means, there is no intrusion. On the off chance that the rank is more than 1 method might be there is an intrusion or not. To discover is there any intrusion or not we are utilizing the profound learning grouping method.

B.Deep learning

The proposed deep learning model uses directed preparing and twofold order for recognizing pernicious exercises. On the off chance that the DNN distinguishes an obscure anomaly or a zero-day assault, it stores the comparing tuples of the separated highlights to the 'Reserve' as feedback. This feedback component is utilized during the retraining of the DNN, which improves the element extraction and naming usefulness of the detection system. Be that as it may, if the removed highlights are not adequate to group the network traffic, feedback is sent to the information assortment and transmission module for retraining.

a. Training Deep Neural Network

DBN is a generative neural networks model comprising of different of stochastic latent variables and hidden factors. The connection among RBM and DBN are interconnected in light of the fact that making and stacking various RBMs empower. It has many hidden layers to prepare information effectively through the enactments of one RBM for additional preparation stages. The previous hidden layer are used as inputs for the next hidden layer. A schematic representation of a DBN based Deep Neural Network is shown in Figure 1. Looking by stacking RBM methodology is based on the layer by layer techniques. It came out by either Gaussian-Bernoulli RBM or Bernoulli–Bernoulli RBM. Here the Bernoulli – Bernoulli RBM is defined by binary variables, but GBRBM (Gaussian-Bernoulli RBM) is defined by nonstop value data.

Given visible units V_i and Unseen units h_j,

Then GBRBM is defined as

$$E(v,h) = -\sum_{i=1}^{n}\sum_{j=1}^{n} w_{ij} h_j \frac{v_i}{\sigma_i} - \sum_{i=1}^{n} \frac{(v_i - a_i)^2}{2\sigma_i^2} - \sum_{j=1}^{m} b_j h_j \quad (5)$$

Where, σ_i is the standard deviation related to V_i.Looking by other logical images are similar to the Bernoulli – Bernoulli RBM. Prohibitive probabilities are described as in the underneath conditions;

$$p(V_i = v/h) = N(V/a_i + \sum_j W_{ij}\, \sigma_i^2) \quad (6)$$

$$p(h_j = 1/v) = f(b_j + \sum_i W_{ij} \frac{v_i}{\sigma_i^2} \quad (7)$$

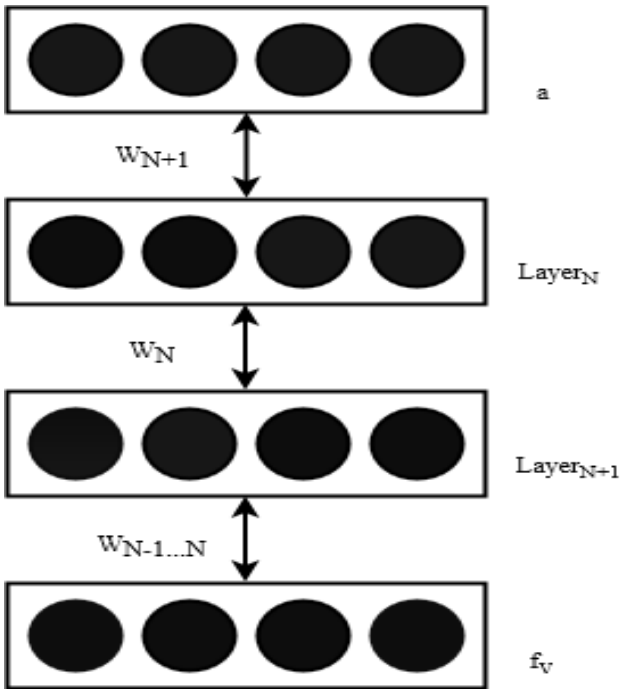

Figure 1: DBN based Deep Neural Network Structure

Algorithm: Trust based classification

a) Begin
b) Initialize number of nodes
c) Forward sample packets to target
d) Calculate satisfactory factor using table 1
e) Calculate the packet based trust using eqn (1)
f) Calculate the feedback based trust using eqn (2)
g) Calculate the total trust of the node using eqn (3)
h) Perform ranking process
a. If T_i^j(Total)>0.9
i. Rank 1
b. Else
i. Rank 2
i) Input rank 2 nodes to deep learning classification
j) Train DNN
k) Output classified results
l) End

IV. SIMULATION RESULTS

This section deals about the experiment setup and result analysis.

A.Dataset for network anomaly detection

As far as we could possibly know, two datasets, for example, KDD-Cup 1999 dataset with NSL-KDD dataset have been employed for preparing and testing datasets. Here the segment, of both the datasets will be quickly depicted.

NSL-KDD dataset isn't latest, yet it was developed because of the weakness of the KDD-Cup 1999 dataset. Science the KDDCup 1999dataset contains the colossal measure of excess records, roughly 75 and 78% are copied in the testing and preparing dataset, it makes the learning algorithm partial. To unravel such problem, NSL-KDD, another adaptation of KDD-Cup 1999 datasets, is generally received for abnormality detection. The NSL-KDD dataset contains four documents, two records for preparing ("KDD-Train+" and "KDDTrain_20 %") and the other two for testing ("KDD-Test+" and "KDDTest-21").

B. Results

In this area we instate five hubs to assess the trust esteems. In the wake of finding the absolute trust esteems we rank the hubs. Based on the positioning we characterize the hubs. Tables 3 speak to the trust esteems.

Table 3: Trust values using Deep Learning Classification

Trust Value	Rank	Classification
0.9592	1	Non intruded
-0.9953	2	May be intruded
-0.9976	2	May be intruded
-0.9984	2	May be intruded
-0.9988	2	May be intruded

On the off chance that the trust esteems is beneath one method there is an opportunity for happening intrusion. To order the intrusion we proposed the deep learning classification.

C.Performance Evaluation Metrics

In our model, the most huge introduction pointer (Accuracy, AC) of intrusion detection is used to check the show of the Proposed-IDS model. Notwithstanding the precision, we present the recognition rate and bogus positive rate. The True Positive (TP) is proportional to those accurately dismissed, and it indicates the number of abnormality records so as to be distinguished as an anomaly. The False Positive (FP) is what might be compared to erroneously dismissed, and it indicates the number of ordinary records that are recognized as an anomaly. The True Negative (TN) is equal to those accurately conceded, and it means the number of typical records that are recognized as would be expected.The False Negative (FN) is identical to those erroneously conceded, and it indicates the number of abnormality records so as to be distinguished as would be expected.

Table4: Values of TN, TP, FN, FP for Deep learning and ANN

Measures	Deep Learning	ANN
TN	10	9
TP	1	1
FN	1	2

FP	2	2

Table 4 shows the correlation between Deep Learning and ANN arrangement based on recognition rate and false-positive rate. Contrasting with ANN Deep learning shows better outcomes. We assessed the detection system by estimating the presentation measurements: Accuracy, TPR, and FPR. The performance of the proposed IDS model is compared with the performance of the ANN algorithm and Deep Learning algorithm in this section in terms of accuracy, TPR and FPR. Exactness: the level of the number of records arranged effectively versus complete the records appeared in(8)

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (8)$$

Table5: Comparison between Classification algorithms based on accuracy

Algorithm	Accuracy (%)
ANN	71.42
Deep Learning	78.54

Table 5 speaks to the exactness correlation between both grouping algorithms.

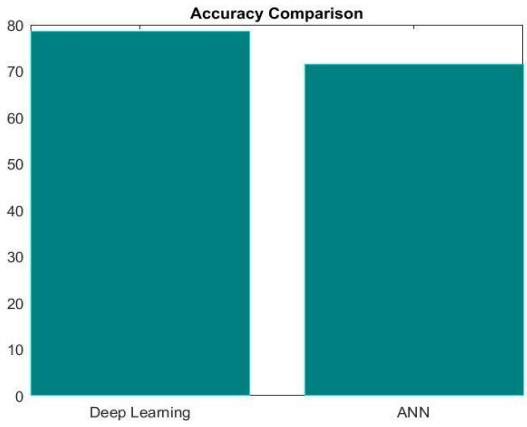

Fig. 2: Accuracy Comparison

Figure 2 shows the exactness of the inspection among the proposed IDS model and the ANN algorithm. Figure 2 shows the exactness of the deep learning-based proposed IDS model is 78.54% and the ANN calculation achieves 71.42% precision with the NSL-KDD dataset.. This shows the centrality of the proposed IDS model than the current IDS models. True Positive Rate (TPR): as what could be compared to the Detection Rate (DR), it shows the level of the number of records recognized effectively over the all sum amount of abnormality records, as appeared in (9).

$$TPR = \frac{TP}{TP+FN} \quad (9)$$

Table6: Comparison between Classification algorithms based on TPR

Algorithm	TPR
Deep Learning	0.5
ANN	0.33

Table 6 speaks to the TPR examination between both grouping algorithms. Figure 3 shows the TPR correlation between deep learning-based proposed IDS model and ANN algorithm.

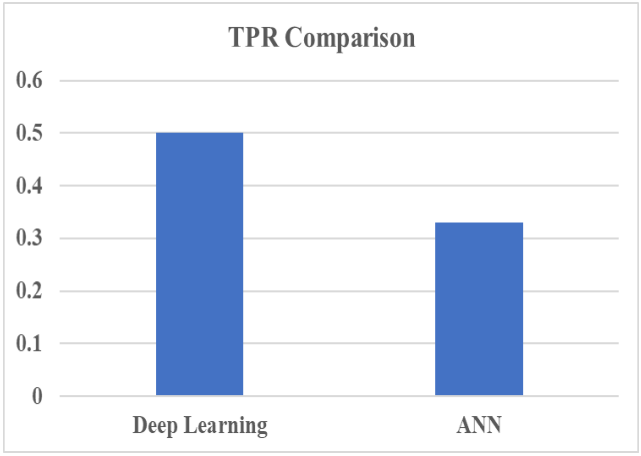

Fig.3: TPR Comparison

Figure 3 shows the TPR of deep learning-based proposed IDS model is ranging 0.5 and the ANN calculation accomplishes 0.33 with the NSL-KDD dataset. The noteworthy contrast in TPR shows the proposed IDS model is proficient.

False Positive Rate (FPR): the degree of the amount records rejected erroneously is detached by irrefutably the number of conventional records, as showed up in (10).

$$FPR = \frac{FP}{FP+TN} \quad (10)$$

Table 7: Comparison between Classification algorithms based on FPR

Algorithm	FPR
Deep Learning	0.16
ANN	0.1818

Table 7 speaks to the examination between both deep learning just as order calculations based on False Positive Rate. Figure 4 shows the FPR examination between deep learning based proposed IDS model and ANN calculation.

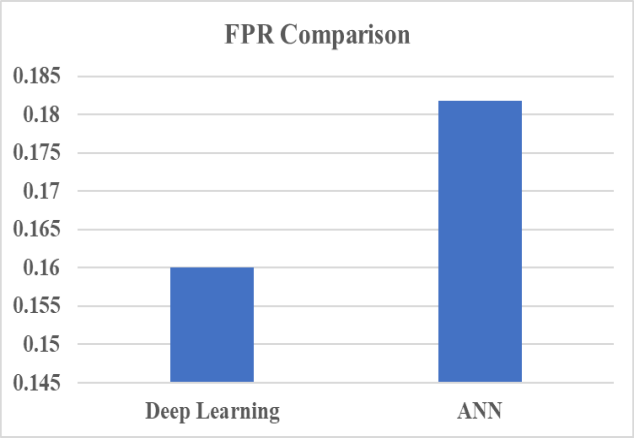

Fig. 4: FPR Comparison

The above figure 4 shows the FPR of the proposed IDS model is extending 0.16 and the ANN algorithm accomplishes 0.1818 with the NSL-KDD dataset. The huge contrast in FPR shows the proposed IDS model is effective.In this manner, the motivation for the IDS is to obtain a higher precision and location rate with a lower false-positive rate

V. CONCLUSION

In this paper, we researched deep learning systems utilized for network intrusion detection, with the developing thoughtfulness regarding deep learning now daily in numerous zones. An outline of Intrusion finding procedures have been presented with the subjects of information decrease, dimensionality decrease, characterization, just as a gathering of deep learning methods. Through investigation of exactness, TPR and FPR, we got a normal precision rate 78.54% for various situations.

REFERENCES

1. Khorshed, MdTanzim, ABM Shawkat Ali, and Saleh A. Wasimi. "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing." *Future Generation computer systems* 28, no. 6 (2012): 833-851.
2. Patcha, Animesh, and Jung-Min Park. "An overview of anomaly detection techniques: Existing solutions and latest technological trends." *Computer networks* 51, no. 12 (2007): 3448-3470.
3. Lee, Wenke, Rahul A. Nimbalkar, Kam K. Yee, Sunil B. Patil, Pragneshkumar H. Desai, Thuan T. Tran, and Salvatore J. Stolfo. "A data mining and CIDF based approach for detecting novel and distributed intrusions." In *International Workshop on Recent Advances in Intrusion Detection*, pp. 49-65. Springer, Berlin, Heidelberg, 2000.
4. Liao, Hung-Jen, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. "Intrusion detection system: A comprehensive review." *Journal of Network and Computer Applications* 36, no. 1 (2013): 16-24.
5. Verwoerd, Theuns, and Ray Hunt. "Intrusion detection techniques and approaches." *Computer communications* 25, no. 15 (2002): 1356-1365.
6. Ravale, Ujwala, NileshMarathe, and Puja Padiya. "Feature selection based hybrid anomaly intrusion detection system using K means and RBF kernel function." *Procedia Computer Science* 45 (2015): 428-435.
7. Furnell, Steven M., P. S. Dowland, H. M. Illingworth, and Paul L. Reynolds. "Authentication and supervision: A survey of user attitudes." *Computers & Security* 19, no. 6 (2000): 529-539.
8. Perdisci, Roberto, Giorgio Giacinto, and Fabio Roli. "Alarm clustering for intrusion detection systems in computer networks." *Engineering Applications of Artificial Intelligence* 19, no. 4 (2006): 429-438.
9. Bolzoni, Damiano, and Sandro Etalle. "Approaches in anomaly-based network intrusion detection systems." *Intrusion Detection Systems* 38 (2008): 1-15.
10. Davis, Jonathan J., and Andrew J. Clark. "Data preprocessing for anomaly based network intrusion detection: A review." *computers & security* 30, no. 6-7 (2011): 353-375.
11. Jin, Xin, and Sylvia L. Osborn. "Architecture for data collection in database intrusion detection systems." In *Workshop on Secure Data Management*, pp. 96-107. Springer, Berlin, Heidelberg, 2007.
12. Peddabachigari, Sandhya, Ajith Abraham, CrinaGrosan, and Johnson Thomas. "Modeling intrusion detection system using hybrid intelligent systems." *Journal of network and computer applications* 30, no. 1 (2007): 114-132.
13. Wang, Ke, and Salvatore J. Stolfo. "Anomalous payload-based network intrusion detection." In *International Workshop on Recent Advances in Intrusion Detection*, pp. 203-222. Springer, Berlin, Heidelberg, 2004.
14. Gowrison, G., K. Ramar, K. Muneeswaran, and T. Revathi. "Minimal complexity attack classification intrusion detection system." *Applied Soft Computing* 13, no. 2 (2013): 921-927.
15. Krishnan, Deepa, and Madhumita Chatterjee. "An adaptive distributed intrusion detection system for cloud computing framework." In *International Conference on Security in Computer Networks and Distributed Systems*, pp. 466-473. Springer, Berlin, Heidelberg, 2012.
16. Aydın, M. Ali, A. Halim Zaim, and K. GökhanCeylan. "A hybrid intrusion detection system design for computer network security." *Computers & Electrical Engineering* 35, no. 3 (2009): 517-526.
17. Valeur, Fredrik, Giovanni Vigna, Christopher Kruegel, and Richard A. Kemmerer. "Comprehensive approach to intrusion detection alert correlation." *IEEE Transactions on dependable and secure computing* 1, no. 3 (2004): 146-169.
18. Jaisankar, N., SannasiGanapathy, P. Yogesh, Arputharaj Kannan, and Kumar Anand. "An intelligent agent based intrusion detection system using fuzzy rough set based outlier detection." In *Soft computing techniques in vision science*, pp. 147-153. Springer, Berlin, Heidelberg, 2012.
19. Depren, Ozgur, Murat Topallar, EminAnarim, and M. Kemal Ciliz. "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks." *Expert systems with Applications* 29, no. 4 (2005): 713-722.

AUTHORS PROFILE

Josemila Baby, She received her master degree in computer Science from Alagappa University, Karaikkudi**.** Currently she is persuing her Doctoral Degree in the Department of Computer Applications in Noorul Islam Centre for Higher Education, Kumarcoil, Nagercoil, India. Her area of research area is networking.

J. R. Jeba, She has completed her Doctoral Degree in the research field of Data Mining in Mother Thresa University, Kodaikanal. Currently working as an Associate Professor & Head in the Department of Computer Applications in Noorul Islam Centre for Higher Education, Kumarcoil, Nagercoil, India. She has published many research articles under her name. Several students are doing Doctoral program under her guidance. She has an extensive record of teaching for more than 22 years.