© 2019 IJSRST | Volume 6 | Issue 3 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology
DOI : 10.32628/IJSRST196315

Intrusion Detection System using Intelligent Deep Boltzmann Machine

K.Veena[1], Prof. P.Damodharan [2], Dr. N. Suguna[3]
[1]PG Scholar, [2]Associate Professor, [3]Professor
Akshaya College of Engineering and Technology, Kinathukadavu, Coimbatore, Tamil Nadu, India

ABSTRACT

In the wireless communication identifying the attacks and ensuring the data/information security is the primary role played by the Intrusion Detection System. In an uncompromised network the network traffic monitored at these two different points in the network should be identical. If differences are detected in the data transmission this may indicate an intrusion of the computer network. The IDS System performs the vital role for the security of the network, consist of three main components: data collection, feature selection/conversion and decision engine. Data preprocessing provides high-quality data for subsequent processing, then different type of feature is extracted from the processed data as vector. The performance is evaluated using the network analysis metrics such as key generation delay, key sharing delay and the hash code generation time for both MLSDN and the proposed Deep Learning (DLSDN). The evaluation shows that the proposed system achieves the better performance in the credential generation processing and in the malicious nodes validation.

Keywords : IDS System, MLSDN, Deep Learning, KDD

I. INTRODUCTION

NETWORK SECURITY

A series of devices or computing nodes interconnected by communication link that allow to share and exchange the data among all devices is defined by the term 'Network'. A device can be anything which is capable of sending or receiving the data that is generated by the device and that is exchanged over the medium or channel. In other words, more than one autonomous computer is grouped together to exchange the information using the communication channel is called as 'Network'. In computer networks, the following characteristics or factors are mainly used to classify the various types of networks.

INTRUSION DETECTION SYSTEM

An Intrusion detection system is an active process or device that analyzes system and network activity for unauthorized entry or malicious activity. The ultimate aim of any IDS is to catch perpetrators in the act before they do real damage to resources. An IDS protects a system from attack, misuse, and compromise. It can also monitor network activity, audit network and system configurations for vulnerabilities, analyze data integrity, and more. Intrusion detection system is software that automates the intrusion detection process. The primary responsibility of IDS is to detect unwanted and malicious activities.

II. METHODS AND MATERIAL

MODEL BASED INTRUSION DETECTION

It states that certain scenarios are inferred by certain other observable activities. If these activities are monitored, it is possible to find intrusion attempts by looking at activities that infer a certain intrusion scenario. The model-based scheme consists of three important modules. The anticipator uses the active models and the scenario models to try to predict the next step in the scenario that is expected to occur. A scenario model is a knowledge base with specifications of intrusion scenarios. The planner then translates this hypothesis into a format that shows the behavior, as it would occur in the audit trail. It uses the predicted information to plan what to search for next. The interpreter then searches for this data in the audit trail. The system proceeds this way, accumulating more and more evidence for an intrusion attempt until a threshold is crossed; at this point, it signals an intrusion attempt.

MACHINE LEARNING

Machine learning is the scientific field dealing with the ways in which machines learn from experience. For many scientists, the term "machine learning" is identical to the term "artificial intelligence", given that the possibility of learning is the main characteristic of an entity called intelligent in the broadest sense of the word Knowledge discovery in databases (KDD) is a field encompassing theories, methods and techniques, trying to make sense of data and extract useful knowledge from them. It is considered to be a multistep process (selection, preprocess, transformation, data mining, interpretation-evaluation). KDD is the nontrivial process identifying valid, novel, potentially useful, and ultimately understandable patterns in data.

Types of Machine Learning Techniques

The machine learning offers a worthy approach for the analysis of high dimensional and multimodal bio-medical data by preparing classy and automatic algorithms. There are various types of machine learning techniques as shown in fig 1.2. Supervised, Unsupervised, Semi Supervised, Reinforcement, Evolutionary Learning and Deep Learning are the types of machine learning techniques. These techniques are used to classify the data set.

1) Supervised learning: It offers a training set of examples with suitable targets and algorithms will respond correctly to all feasible inputs on the basis of this training set. Learning from exemplars is another name of Supervised Learning. The supervised learning are classified into two types, Classification and regression. Classification: It gives the prediction of Yes or No, for example, "Is this tumor cancerous?" Regression: It gives the answer of "How much" and "How many".

2) Unsupervised learning: In unsupervised learning correct responses or targets are not provided. It tries to find out the similarities between the input data and based on these similarities, un-supervised learning technique classify the data. This is also known as density estimation. Unsupervised learning includes clustering. Clustering: it makes clusters on the basis of similarity.

3) Semi supervised learning: Semi supervised learning technique is a class of supervised learning techniques. This learning also used unlabeled data for training purpose (generally a minimum amount of labeled-data with a huge amount of unlabeled-data). Semi-supervised learning lies between unsupervised-learning (unlabeled-data) and supervised learning (labeled-data).

4) Reinforcement learning: This learning is encouraged by behaviorist psychology. When the answer is wrong, the algorithm is informed but does not inform the way to correct it. It has to explore and test various possibilities until it finds the right answer. It is also known as learning with a critic. It does not recommend improvements. Since Reinforcement learning neither offers accurate input and output nor suboptimal actions, it is different from supervised learning. Moreover, it focuses on on-line performance.

III. LITERATURE SURVEY

Mathematical optimization (Sheth et al, 2016) is the technique which processes the function of several inputs under the set of constraints either by using the linear programming or by using the system analysis to select the best set of solution. The selection of best combination is identified in maximum or minimum based on the problem category. Mainly optimization is used to determine the best combination among all possible combinations, by applying reduction in the number of iterations which avoids the processing of entire solution sets using the cognitive ability. Deep belief network pre-training was the first pre-training method to be widely studied, although many other techniques now exist in the literature. That deep auto-encoders could be trained effectively using deep belief net pre-training, there was a resurgence of interest in using deeper neural networks for applications. Although less pathological deep architectures than deep auto-encoders can in some cases be trained without pre-training, for many problems and model architectures, researchers have reported pre-training to be helpful. We view the various unsupervised pre-training techniques as convenient and robust ways to help train neural networks with many hidden layers that are generally helpful, rarely hurtful, and sometimes essential.

Zhenzhen jiao et al (2000) surveyed the back pressure based routing strategies for multi-hop wireless networks. Dynamic topology, delay based backpressure, queue based, cross layer back pressure algorithm are surveyed for both static and dynamic wireless networks. This model with sustained optimization of throughput was developed by Majed Alresaini et al (2000) by validating traffic conditions in the mobile networks. The hybrid model provide the distributed knowledge about the wireless devices in the various network load conditions. Adaptive redundancy with efficient energy handling provide the dynamic connectivity in sparse and highly dynamic network.

Multi-hop communication and the adaptation to improve the communication reliability are studied by Yu-Chee Tseng et al (2003) to avoid the flooding problem in MANET. Broadcast storm problem in the multi-hop wireless network causes the contention, redundancy of message, and collision in the network. The adaptation of the design, is done by dynamically adjusting the threshold based on local connectivity information.

SSL Certificates have a key pair: a public and a private key. Device connects to a web server (website) secured with SSL (https). Device requests that the server identify itself. Server sends a copy of its SSL Certificate, including the server public key. Device checks the certificate root against a list of trusted CAs and that the certificate is unexpired, unrevoked, and that its common name is valid for the website that it is connecting to. If the Device trusts the certificate, it creates, encrypts, and sends back a symmetric session key using the servers public key. Server decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session. Server and

Device now encrypt all transmitted data with the session key.

The cryptographic parameters of the session state are produced by the SSL handshake protocol, which operates on top of the SSL record layer. When an SSL client and server first start communicating, they agree on a protocol version, select cryptographic algorithms, optionally authenticate each other, and use public key encryption techniques to generate shared secrets. These processes are performed in the handshake protocol, which can be summarized as follows: the client sends a client hello message to which the server must respond with a server hello message, or else a fatal error will occur and the connection will fail. The client hello and server hello are used to establish security enhancement capabilities between client and server. The client hello and server hello establish the following attributes: Protocol Version, Session ID, Cipher Suite, and Compression Method. Additionally, two random values are generated and exchanged: ClientHello. random and ServerHello. random.

Cognitive systems using the perceptual learning by the mathematical engineering are surveyed by Yingxu Wang et al, 2017. The survey discussed about the theory about the abstract intelligence with the natural and computational intelligence. The triggered application of the abstract intelligence in various fields such as cognitive computers, cognitive robots, cognitive neural networks and cognitive learning are presented with the advantage of the Brain-Inspired Systems. The framework of the intelligence science is integrates the exploration of the Neuroinformatics, Braininformatics, Cognitiveinformatics and the artificial intelligence with the denotational mathematics.

The Genetic Algorithm is a biologically inspired heuristic search technique based on the phenomenon of natural genetics. The GA maintains the population of individuals that characterize the candidate solutions to the given problem. Each individual chromosome in the population is evaluated to find its fitness level (how much it is close to the optimal solution) from the given objective functions. The chromosomes consist of different genes and these genes can be represented through the binary numbers [0,1].The complexity of chromosome is directly depends upon the number of genes and the bits/gene.

The GA performs well for large search space problems because it can work on a population in parallel instead of processing a single solution at a time. The parallel processing allows the GAs to explore several parts of the solution at same time and also many real world problems require simultaneous optimization of several objective functions. Hence, these algorithms become suitable to solve these problems. However, the objective functions may have conflict in their objectives. These contradictory requirements of different objective functions give rise to a set of possible solutions call pareto optimal solutions instead of a single possible solution. The main reason for the multiple possible solutions is that no single solution can be thought as the best one than the other solution in the optimal set. The working of GA can be described by the Steps.

- Initialize the population of chromosomes.
- Compute the fitness level of each chromosome to rank them.
- Select the best chromosomes in terms of their fitness.
- Perform the crossover operation on selected chromosomes.

- Perform the mutation function on selected chromosomes.

If stopping criteria is achieved terminate the GA otherwise move to step 2 of the algorithm.

IV. IMPLEMENTATION

Implementing and using SSL to secure HTTP traffic

Security of the data stored on a file server is very important these days. Compromised data can cost thousands of dollars to company. In the last section, compiled LDAP authentication module into the Apache build to provide a Authentication mechanism. However, HTTP traffic is very insecure, and all data is transferred in clear text - meaning, the LDAP authentication (userid/passwd) will be transmitted as clear text as well. This creates a problem. Anyone can sniff these userid/passwd and gain access to DAV store. To prevent this encrypt the HTTP traffic is essentially as HTTP + SSL or HTTPS. Anything transferred over HTTPS is encrypted, so the LDAP userid/passwdcan not be easily deciphered. HTTPS runs on port 443. The resulting build from the last section's compilation process will have Apache to listen to both port 80 (normal HTTP) and 443 (HTTPS). If you are just going to use this server for DAV, then I will highly suggest that you close port 80. In this section of the HOWTO I will provide some information regarding SSL and maintaining SSL on a Apache HTTP server

Symmetric Cryptography - Actual transmission of data: After the SSL connection has been established, Symmetric cryptography is used for encrypting data as it uses less CPU cycles. In symmetric cryptography the data can be encrypted and decrypted using the same key. The Key for symmetric cryptography is exchanged during the initiation process, using Public Key Cryptography.

Message Digest The server uses message digest algorithm such as HMAC, SHA-1, MD5 to verify the integrity of the transferred data.

Ensuring Authenticity and Integrity

Encryption

Step1: In this step the Original "Clear Text" message is encrypted using the Sender's Private Key, which results in Cipher Text 1. This ensures the Authenticity of the sender.

Step2: In this step the "CipherText 1" is encrypted using Receiver's Public Key resulting in "CipherText 2". This will ensure the Authenticity of the Receiver i.e. only the Receiver can decipher the Message using his Private Key.

Step3: Here the SHA1 Message Digest of the "Clear Text" is created.

Step4: SHA1 Message Digest is then encrypted using Sender's Private Key resulting in the Digital Signature of the "ClearText". This Digital Signature can be used by the receiver to ensure the Integrity of the message and authenticity of the Sender.

Step5: The "Digital Signature" and the "CipherText 2" are then sent to the Receiver.

Decryption

Step1: In this step the "CipherText 2" message is decrypted using the Receiver's Private Key, which results in Cipher Text 1.

Step2: In this step the "CipherText 1" is decrypted using Sender's Public Key resulting in "ClearText".

Step3: Here the SHA1 Message Digest of the "Clear Text" is created.

Step4: The "Digital Signature" is then decrypted using Sender's Public Key, resulting the "SHA 1 MSG Digest".

Step5: The "SHA1 MsgDigest #1" is then compared against "SHA1 MsgDigest #2". If they are equal, the data was not modified during transmission, and the integrity of the Original "Clear Text" has been maintained

The client hello and server hello are used to establish security enhancement capabilities between client and server. The client hello and server hello establish the following attributes: Protocol Version, Session ID, Cipher Suite, and Compression Method. Additionally, two random values are generated and exchanged: ClientHello.random and ServerHello.random.

Machine Learning

The cognitive architecture operates based on the generic rules with the intelligence of the knowledge processing using the biologically inspired computing. The learning and knowledge processing system is developed by using the intelligent agent with the artificial computational process based on the unified theory of cognition. The problem solving competence with the knowledge representation for the information processing is associated based on the human associative theory. The proposed model is developed based on the Cognitive Behavioral Theory (CBT) which describes the role of cognition to explore the current situation and performing the behavioral pattern using the observational learning. It mainly retrieves the extrinsic and intrinsic factor which affects the interpretation and information processing.

V. RESULT AND DISCUSSION

7.1 OPERATIONAL ENVIRONMENT

The real world testing process is done in C#.net environment by running the working design using the validation metrics. This analysis is used to test the performance of the existing protocols as well as newly derived protocols. Here, the testing is conducted to validate the quality of the proposed protocol, which is designed to improve the scalability network protocols. The performance evaluation is conducted to validate the execution of the proposed technique in terms of packet related metrics such as key generation and key sharing delay, hash code generation delay. The table shows that the parameters used to perform the network performance validation.

Key Generation Delay: Delay refers the average time taken to complete the end to end key generation delay from user device to server in the network using equation (1).

Deep Learning Process

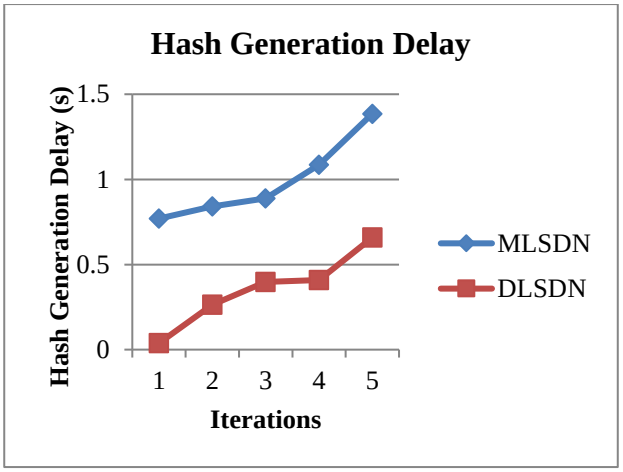
Restricted neural network in deep learning, a stochastic neural network which consists of one layer of visible units and another layer of hidden units and finally the bias unit. In bias unit where the state could be always on and it is a way of adjusting the different inherent of different task. Restricted neural network,it allows only minimum number of network to connect.

1. The DBM structure has to be formed by regulating the network structure into bipartite graph structure.
2. The bipartite graph Structure has set of vertices which are connected by the set of edges with only one relative edge.
3. The term relative edge represents the edge which indicated the connectivity of the vertices and the absence of the particular edge converts the network structure into two graphs.
4. In the bipartite graph, the input layer is form is formed by the nodes in the communication range.
5. The probability of the nodes is distributed using the Bernoulli distribution.
6. The hidden layer vector is associated by maintaining the connection between each input in the hidden layer to the current node
7. The value vector of the hidden layer is regulated by checking the values of the probability of connection in the partition function.
8. The output of the partition function is validated for the conditional probability.

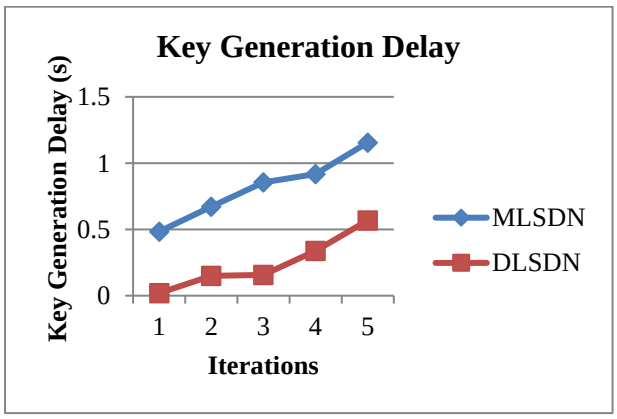
9. The condition probability is used to derived the individual activation probability
10. The activation function requires the logistic sigmoid and the softmax function

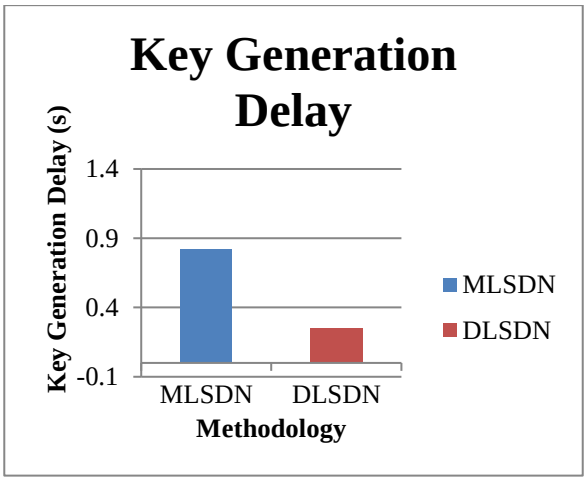
PERFORMANCE EVALUATION

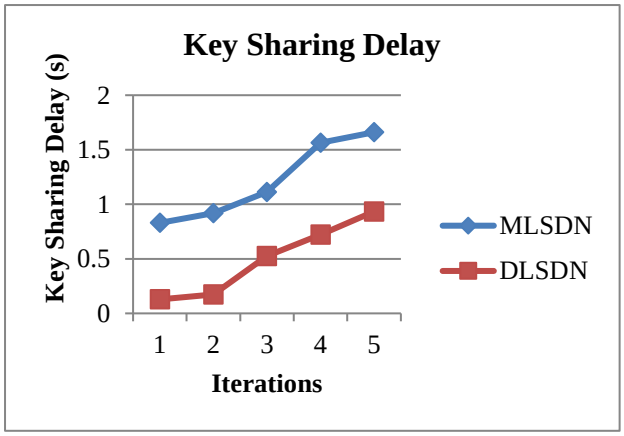
Figure 1, 2 and 3 shows the comparisons between MLSDN and Deep Learning Software Defined Network in terms of Key Generation Delay, Key Sharing Delayand Hash Generation Delay respectively. It outcomes in key generation process and key sharing process. In case of Key Generation Delay, DLSDNachieveshigher performance by obtaining the lower delay. Similarly for Key SharingDelay DLSDNin lower latency compare to MLSDN. In case of Hash Generation Delay, DLSDN achieves lower delay while generating the hash code.

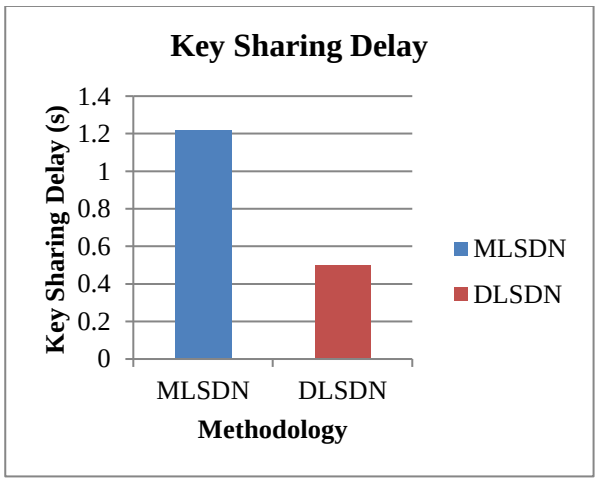


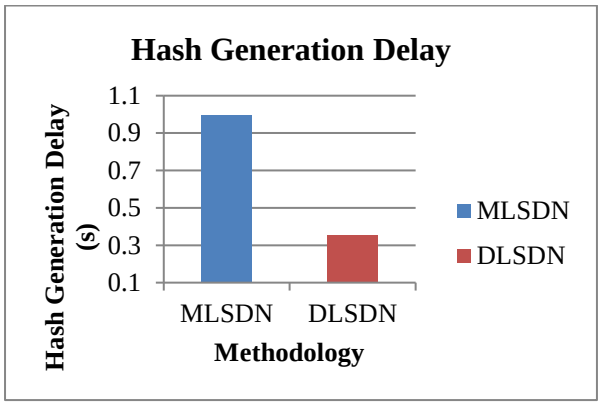
the average performance comparisons between MLSDN and DLSDN in terms of Key Generation Delay, Key Sharing Delayand Hash Generation Delay respectively.











The performance analysis shows that the proposed deep learning technique achieves better performance compare to the existing machine learning based software defined network in terms of delay in Key Generation, Key Sharing and Hash Generation Delay

VI. CONCLUSION

The Deep Learning based SDN model is the novel networking model which utilizes the packet forwarding and an attacker detection system. The proposed architecture enhances the network resilient, decompose management complexity by enforcing the network policy enforcement. The proposed intrusion detection system is mostly placed at strategic points in a network, so that it can monitor the traffic traveling to or from different devices on that network. The proposed IDS system analyzes the network activity for unauthorized entry or malicious activity using the deep learning. The system performs the learning process about the normal and anomalous behavior by analyzing network traffic, which is used to predict unknown and new attacks. Proposed system that analyzes the traffic crossing the network and validates the payload by comparing the data transmission with the trained pattern using the Deep Learning.The evaluation showed that the proposed system achieved better performance in terms of Key Generation Delay, Key Sharing Delay and Hash Code Generation Delay.

VII.FUTURE WORK

It can enhance for multimedia data transmission and for sharing the data over the cloud communication. Compliance with real-time constraints: In real-time applications, data is delay-constrained and has a certain bandwidth requirement. For instance, scheduling messages with deadlines is an important issue in order to take appropriate actions in real time. However, due to the interference and contention on the wireless medium, this is a challenging task. Multi-channel communication can help to reduce the delay by increasing the number of parallel transmissions and help the network to achieve real-time guarantees. Assignment of overlapping channels during run-time: Use of overlapping channels at run time during medium access is an interesting and challenging future research direction.

VIII. REFERENCES

[1]. Khoshkbarforoushha, R. Ranjan, R.Gaire, E. Abbasnejad, L. Wang, and A. Y. Zomaya. Distribution based workload modelling of continuous queries in clouds. IEEE Transactions on Emerging Topics in Computing,5(1):120–133, 2017

[2]. Benaloh.J, “Key Compression and Its Application to Digital Fingerprinting” technical report, Microsoft Research, 2009.

[3]. D. D´ıaz-Pernil, A. Berciano, F. Pe˜na-Cantillana, and M. A. Guti´errez- Naranjo. Bio-inspired parallel computing of representative geometrical objects of holes of binary 2d-images. International Journal of Bio-Inspired Computation, 9(2):77–92, 2017.

[4]. Chen, F., Ji, R., Su, J., Cao, D. and Gao, Y., 2018. Predicting Microblog Sentiments via Weakly Supervised Multimodal Deep Learning. IEEE Transactions on Multimedia, 20(4), pp.997-1007.

[5]. Jiang, F., Fu, Y., Gupta, B.B., Lou, F., Rho, S., Meng, F. and Tian, Z., 2018. Deep Learning based Multi-channel intelligent attack detection for Data Security. IEEE Transactions on Sustainable Computing.

[6]. G.-G. Wang, X. Cai, Z. Cui, G. Min, and J. Chen. High performance computing for cyber physical social systems by using evolutionary multi-objective optimization algorithm. IEEE Transactions on Emerging Topics in Computing, 2017. [26] L. Wang, H. Geng, P. Liu, K. Lu, J. Kolodziej, R. Ranjan,

[7]. J. Kim, N. Shin, S. Y. Jo, and S. H. Kim, "Method of intrusion detection using deep neural network," in Big Data and Smart Computing (BigComp), 2017 IEEE International Conference on. IEEE, 2017,

[8]. L. Liu, L. Shao, X. Li, and K. Lu, ``Learning spatio-temporal represen-tations for action recognition: A genetic programming approach,'' IEEETrans. Cybern., vol. 46, no. 1, pp. 158_170, Jan. 2016.[4] A.-A. Liu, Y.-T. Su, W.-Z. Nie, and M. Kankanhalli, ``Hierarchical cluster-ing multi-task learning for joint human action grouping and recognition,''IEEE Trans. Pattern Anal. Mach. Intell., vol. 39, no. 1, pp. 102_114,Jan. 2017

[9]. Lei, L., You, L., Dai, G., Vu, T.X., Yuan, D. and Chatzinotas, S., 2017, August. A deep learning approach for optimizing content delivering in cache-enabled HetNet. In Wireless Communication Systems (ISWCS), 2017 International Symposium on (pp. 449-453). IEEE.

[10]. Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y. and Gan, D., 2018. Cloud-based cyber-physical intrusion detection for vehicles using Deep Learning. IEEE Access, 6, pp.3491-3508.

[11]. Y. Ye, T. Li, D. Adjeroh, and S. S. Iyengar. A survey on malware detection using data mining techniques. ACM Computing Surveys(CSUR), 50(3):41, 2017.

[12]. Z. Cui, B. Sun, G. Wang, Y. Xue, and J. Chen. A novel oriented cuckoo search algorithm to improve dv-hop performance for cyber–physical systems. Journal of Parallel and Distributed Computing, 103:42–52, 2017.

Cite this article as :

K. Veena, Prof. P. Damodharan, Dr. N.Suguna, "Intrusion Detection System using Intelligent Deep Boltzmann Machine", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 6 Issue 3, pp. 78-86, May-June 2019.

Journal URL : http://ijsrst.com/IJSRST196315