ISSN 2409-2665
Journal of Logistics, Informatics and Service Science
Vol. 9 (2022) No.2, pp. 118-130
DOI:10.33168/LISS.2022.0207

Anomaly Detection Using Deep Neural Network Quantum Encoder

S. Madhavi [1] and Seng-Phil Hong [2]

[1] Department of CSE, PVP Siddhartha Institute of Technology, AP, India
[2] Convergence Security MBA, Seoul School of Integrated Science & Technologies, Korea

sphong@assist.ac.kr

Abstract. Quantum computers are replacing the existing classical computers in the very near future time. Due to the evolution of Quantum computers, machine learning techniques are used as a tool for recognizing patterns in the given data. Network security is a major issue nowadays. Many machine learning-based Auto encoders exist for anomaly detection in the network. The Deep learning neural networks based auto encoders increase the accuracy of the anomaly detection models. To implement various machine learning models on a quantum computer the classical data should be converted into qubits. Hence in this paper, we propose a deep neural network-based quantum auto encoder for detecting various network anomalies like Dos, Shellcode, Worm, and Backdoor. Dimensionality reduction is applied to reduce the size of the sample data features set. The proposed method yields high accuracy of 100% during the training phase and 99% during the testing phase.

Keywords: quantum embedding, qubits, anomaly detection, qiskit, fidelity, confusion matrix

1. Introduction

Due to recent advancements in the field of Quantum communications and machine learning researchers had found it useful to apply machine learning concepts to the field of quantum communications. . In various applications the size of data is huge and it needs heavy data storage requirements. Hence much of the research work concentrated on dimensionality reduction to increase the cost efficiency of the computing system.

For example, Feature dimensionality reduction is applied in many pattern recognition applications. Secure quantum communications are very essential in the field of online transactions, monitoring applications, and Business applications. Though many intrusion detection methods exist, the attacker still finds new ways to attack the network and create malicious activities to decrease the efficiency of communications in the network. Basically, these anomalies can be detected by classifying them into classes like abnormal data or Normal data. In this paper, we implemented a novel method that is based on deep neural learning techniques for detecting anomalies in the quantum network. The proposed method detects attacks like DoS, Backdoor, Worms, and Shellcode.

The proposed method first uses quantum embedding techniques to convert classical data to quantum. The model is trained with the features of the normal and abnormal data samples. The proposed model detects anomalies with high accuracy.

This paper proposes a deep neural network-based Quantum Autoenoder DQEN for detecting the attacks like Dos, Backdoor, worms, and shellcodes in the quantum network with high accuracy.

The proposed DQEN is a multilayer neural network that consists of

1, An Encoder to encode the high dimensionality data to low dimensionality data.

2. A Decoder for decoding and recovering the high dimensionality data

3. Bottleneck layer.

In Section II discuss the literature study. In Section III presents the proposed algorithm for Anomaly detection using deep learning neural network based Auto encoder. In Section IV, presents the results. In Section V presents the conclusions and future study.

2. Related Studies

In (Lee et al., 2015; Yeo et al., 2007; Kim et al., 2008; Vaghela, 2020; Golzarnia et al., 2021; Song, et all., 2020; Kim, 2021; Canlas 2021) authors implemented various methods for providing security to various online public services/onine transactions like Health Care System. , Smart Card Protection, Security Practices in Security Management, ATM Cards on Smartphones applciations ,E-commerce applications,

Secure Mobile Payment Architecture,, IOT architectures, Electricity Theft Detection using Fusion DenseNet-RF Model.

In (Pullagujju 2016; Kim et al., 2021; Nooribakhsh et al., 2018; Ibor, et al., 2018; Beg et al., 2021; Rubinstein et al., 2009) authors implemented a methods for identifying malicious activities and enhance security in network communications. In (Kim et al., 2016; Nadella 2016; Divya 2015; David et al., 2021; Lee, 2018; Bhattacharyya et al., 2010; Mandal et al., 2014; Mandal et al., 2014) authors discussed various design architecture for enhancing wireless ad hoc security including IoT, Cloud Platform and Bluetooth Network. In (Kim 2018) authors discussed various Deep Learning Neural Networks for Automatic Vehicle Incident Detection. In (Shin, et al., 2015) authors presented a method for Predicting Software Reliability Using Particle SWARM Optimization Technique. In (Kim, et al., 2016) identified a method for Recognition using Cyber bullying in view of Semantic-Enhanced Minimized Auto-Encoder. In (Li 2019) presented an Extensive Review on Recent Deep Learning Applications. In (Chen, et al., 2020) discussed a Customer Online Shopping Feature Extraction Based on Data Mining Algorithm. In (Patil, et al., 2021) implemented Determining Crime Pattern Based on Clusters Using Guided Population with Dominancy Supported Genetic Algorithm. In (Sarddar, et al., 2017) authors discussed Edge Server Selection in Distributed Content Delivery Network using K-means Square Classification Algorithm and Ant Colony Optimization. In (Olson, et al., 2018) authors presented a Manifold learning techniques for unsupervised anomaly detection. In (Cho, et al., 2018) authors discussed Automated ROI Detection in Left Hand X-ray Images using CNN and RNN. In (Son, et al., 2018) discussed Hybrid Deep Neural Network based Performance Estimation Method for Efficient Offloading on IoT-Cloud Environments. In (Lee, et al., 2018) authors discussed Design of Internet of Things Business Model with Deep Learning Artificial Intelligence. In (Aslam, et al., 2017) authors discussed Hybrid Network Intrusion Detection System Using Machine Learning Classification and Rule Based Learning System. In (Cui, et al., 2016) authors discussed A Sense Embedding of Deep Convolutional Neural Networks for Sentiment Classification. In (Agrawal, et al., 2019) implemented various Ensemble Technique for Intruder Detection in Network Traffic. In (Madhavi, et al., 2021) auhors presented a Secured Quantum Wireless Sensor Network Using IQOTP and Super Dense Coding.In (Papernot, et al., 2015) authors presented a Distillation as a Defense to Adversarial Perturbations against Deep Neural Networks. In (Schmidhuber 2015) authors discussed Deep learning in neural networks: an overview. In (Song 2021) authors implemented a novel deep auto-encoder. In (Hinton, et al., 2006), (Jiang 2016) authors applied dimensionality for reducing the features of data with neural networks, anchor graph and classification for hyperspectral image analysis. In (Schuld, et al., 2020) and (Schuld, et al., 2020) authors implemented quantum classifiers using ensemble techniques. In (Rebentrost,

et al., 2014) presented a Quantum Support Vector Machine for Big Data Classification. In (Mosca, 2018) authors overviewed the need for implementation of Quantum Cybersecurity. In (Torlai, et al., 2020) authors presented a Machine-Learning Quantum States in the NISQ Era.

3. Proposed DQEN Algorithm

The present study proposes a DQEN algorithm which

1. Depends less on the number of training samples
2. Converges to the optimum
3. Results in optimal reliability
4. Minimizes the reconstruction errors.

Compared to the traditional auto encoders

Fig. 1 represents a quantum encoder. Each node represents a qubit. It consists of an input layer which is used for encoding and an output layer for decoding or producing the output.

And all the edges connecting adjacent layers represent a unitary transformation from one layer to another.

Fidelity is used to quantify the difference between the initial state and the final state. The learning task for a quantum auto encoder is to find unitary for detecting anomalies.

Let $F(|\psi_i\rangle, \rho_i^{out}) \approx 1$ for all the input states.

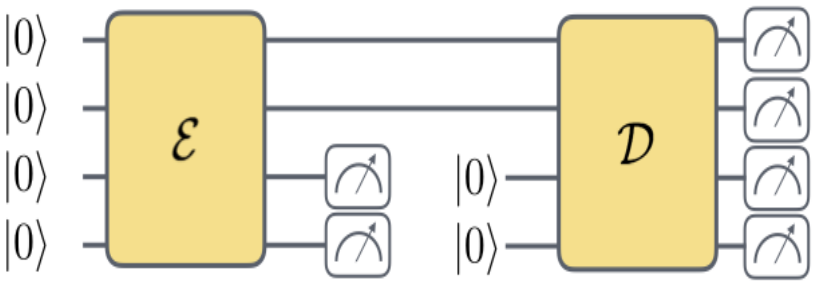

Fig 1: Quantum encoder

The consists of the following phases

1.) Obtain the input classical data

We simulated our network for a period of 3 minutes and Obtained the input data x, Obtain the data. a sample of 3000 data samples for training and 1000 data samples for testing has been obtained.

2.) Training phase: We used a sample of 128 features and 3000 data points having normal and abnormal samples. Dimensionality Reduction is the process of applying Feature Selection using the recursive feature elimination method or Feature Extraction using auto encoders. We applied auto encoders to extract the

meaningful information from the data samples and finally obtained two classes with every 128 features which were reduced to 36 features still. We scaled data from –∏ to +∏ using ensemble techniques. The DQEN is trained to identify any given data sample to either of the known classes. The threshold for the sample is calculated and any sample higher than the threshold is identified as an attack.

Quantum Embedding phase.

In Quantum Communications qubits are used for representing the data. To make the quantum computer process the classical data, the classical data should be mapped to a quantum state. Quantum computers map data to Hilbert space. This mapping is called a quantum feature map. A quantum feature map is prepared from the input data x, a feature map ϕ is defined as $\phi: X \to F$ where F is the feature space. A feature map on n-Qubits is generated. Consider an N-dimensional vector x(m) with N features. To embed this vector into a quantum system we use various embedding techniques. The qubits which represent a quantum state can be encoded by applying a unitary operator. Every classical data is encoded using a set of parameters i.e. a quantum state $|\psi_x\rangle$

A qubit can be embedded using many features into rotation angles, phases of a qubit, and amplitudes of the qubit. In this paper, we used the features to represent the rotation angle of the qubit. The N features are used to represent the

Rotation angle of n qubits here N<= n. the rotation operator is used for encoding Where Θ is the angle for rotation in radians along the x-axis of the Bloc sphere.

$$R_x(\theta) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

3.) Training phase for Detection of intrusions. The deep learning neural network model is used to predict the anomaly. this phase involves in running an a DQEN algorithm to classify data samples as normal or anomalous training data is $\{|\tilde{\psi}_i\rangle, |\psi_i\rangle\}$ i=1..L, ∈ H, where U| is with probability 1 − p and a random pure state sampled from a uniform distribution During this phase the attack samples from the training data set are separated from the normal samples. The DQEN will be trained with the two classes of data like Normal and abnormal data samples.

Let matrix $\rho = \frac{1}{M}\sum_i |\psi_i\rangle\langle\psi_i|$ denotes the density matrix from a set $|\psi_i\rangle$. Let matrix $\sigma = \frac{1}{M}\sum_j |\psi_j\rangle\langle\psi_j|$ denotes the density matrix from a set $|\psi_i\rangle$. Now the fidelity classifier is calculated as $f(\psi) = \langle\psi|\rho - \sigma|\psi\rangle$.

A quantum classifier can prepare and measure quantum states multiple times. If M is the measurable observable then through a set of multiple runs we can estimate the expectation of the M as . $\langle x|M\langle x|$

I.e. $\rho - \sigma = \sum \lambda_j |\psi_j\rangle\langle\psi_j|$ represents the difference between the two density matrix's using their diagonal basis with Eigen values λ_j.

If $P_{\psi=}|\psi\rangle\langle\psi|$ the projection gives a $\langle\phi|P_\psi|\phi\rangle = |\langle\psi|\phi\rangle|^2$ then the vector $|\varphi\rangle$ is equal to a vector $|\psi\rangle$

Let $\prod_+ = \sum_{\lambda_j>0} |\psi_j\rangle\langle\psi_j|$ and $\prod_- = \sum_{\lambda_j<0} |\psi_j\rangle\langle\psi_j|$ are the two projection operators then fidelity is calculated $f(\psi) = \langle\psi|\prod_+ - \prod_-|\psi\rangle$ to find the loss. Finally, the loss should be minimized so that the discrimination between normal and abnormal sets should e identified clearly. Hence train the model until fidelity is less than a threshold value of 0.5.

4. Optimal phase. The optimal measurement depends on this loss and embedding type.

Let U denotes the linear transformation on the embedded inputs $|\psi_i\rangle$. Then the optimal measurement is made by performing $U(\theta)^+ MU(\theta)$

Our objective is to find the unitary U ~p which maximizes the average fidelity, which we define to be the cost function, C1

$$C_1(\vec{p}) = \sum_i p_i . F(|\psi_i\rangle, \rho^{out}_{\vec{i,p}})$$

Thus With the estimates of all the fidelities, the cost function C is computed and fed into a classical optimization routine that returns a new set of parameters for the proposed auto encoder. These steps are repeated until the optimization algorithm converges. Repeat for the next period of time where the training and detection process runs in parallel.

4. Simulation

We tested our model on IBM's quantum computer through Qiskit. Initially, the dimensionality are reduced and the ends at finding the difference between the normal to abnormal after a few epochs with 0.9 accuracies.

The 3000 data samples with 128 features are generated and given to the proposed DQEN auto encoder which reduced the features to 36 in number. The various attacks like Dos, Worm, Shellcode, and backdoor are used for training and testing purposes. The algorithm 1.0 is repeated until the loss is minimized to a value less than 0.5. We obtained 100 accuracies for all the attack types during the training phase. During the testing phase figure, 2.0 shows the TP, TN, FP, FN, recall, precision, and F-score when tested with 1000 testing sample data.

The number of echos is 500 and the learning rate is set as 0.005. Approximately 3000 training pairs which consisting of 36 features are used and at the end of each epoch the fidelity is calculated and the accuracy obtained at the end of the first 130 epochs tested on data is 0.99721 as shown if Figure 3.

Hence the proposed model is trained successfully to identify all attacks with a maximum accuracy of 99%.

The various model testing parameters used in testing the efficiency of the proposed model are as follows

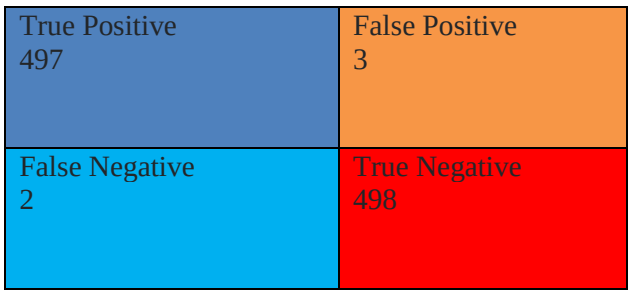

Fig. 2: Confusion matrix

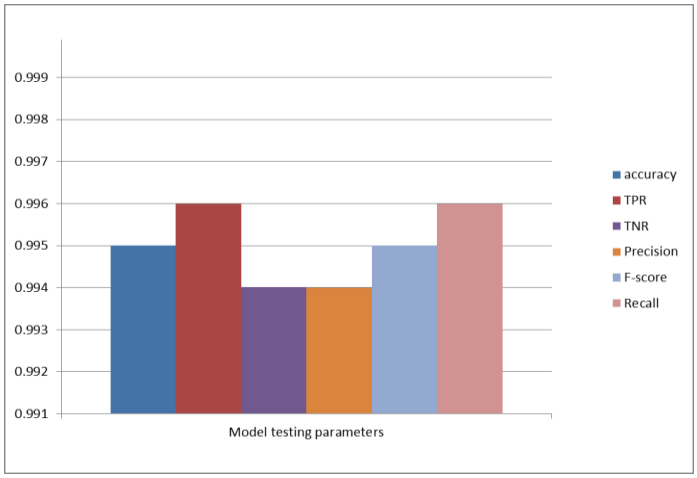

Fig. 3a: Model testing parameters

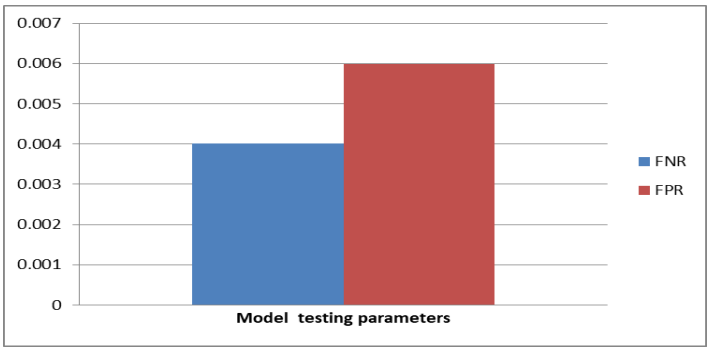

Fig. 3b: Model testing parameters

- True positive rate : TPR=TP/(TP+FN)
- False positive rate : FPR=FP/(FP+TN)
- True negative rate : TNR=TN/(FP+TN)
- False Negative rate : FNR=FN/(FN+TP)
- Precision : TP / (TP + FP)
- Recall = TP / (TP + FN)
- Accuracy = (TN+TP) / (FN+TP+TN+FP)
- f-score / F-Measure = (2 * Precision * Recall) / (Precision + Recall)

Where TP is the number of true positives, FP is the number of false positives, FN is the number of false negatives and TN is the number of true negatives.

5. Conclusion

Our proposed DQEN is successfully implemented and able to differentiate between normal and malicious data samples. It can be used for anomaly detection and obtained an accuracy of 99%. The proposed DQEN can be applied in

application areas like fraud detection, network anomalies with careful initialization of normal to abnormal sample features. The simulation study is implemented using IBM Qiskit environment. In future we wanted to extend the study on entanglement encoders which is helpful for improving the recovery ability of the quantum auto encoders.

References

Abbas, A., Schuld, M., & Petruccione, F. (2020). On quantum ensembles of quantum classi_ers. arXiv: 2001.10833[quant-ph] arXiv: 2001.10833.

Agrawal, A., Mohammed, S., & Fiaidhi, J. (2019). Ensemble technique for intruder detection in network traffic. *International Journal of Security and Its Applications*, NADIA, ISSN: 1738-9976 (Print); 2207-9629 (Online), 13(3), 1-8. DOI: http://dx.doi.org/10.3383 2/ijsia .2019.13.3.01.

Aslam, U., Batool E., Ahsan, S. N. & Sultan, A. (2017). Hybrid network intrusion detection system using machine learning classification and rule based learning system. *International Journal of Grid and Distributed Computing*, NADIA, ISSN: 2005-4262 (Print); 2207-6379 (Online), 10(2), 51-62. DOI: http://dx.doi.org/10.14257/ijgdc.2017.10.2.05.

Beg, S., Zahir, A., Khan, A., & Mohsin, S. (2021). Type 2 heuristics (T2H) in intrusion detection system (IDS): A survey. *International Journal of Security and Its Applications*, NADIA, ISSN: 1738-9976 (Print); 2207-9629 (Online), 15(11), 23-34. DOI: http://dx.doi.org/10.33832 /ijsia.2021.15.1.03.

Bhattacharyya, D., Chakraborty, P., Alisherov, F., & Kim, T. -H. (2010). Quantum watermarking: A review. *International Journal of Security and Its Applications*, NADIA, ISSN: 1738-9976 (Print); 2207-9629 (Online), 4(3), 46-54.

Canlas, R. B. (2021). Capturing security mechanisms applied to ecommerce: an analysis of transaction security. *International Journal of Security and Its Applications*, NADIA, ISSN: 1738-9976 (Print); 2207-9629 (Online), 15(1), 1-10. DOI: http://dx.doi.org/10.33832/ijsia.2021.15.1.01.

Chen, C. -C. & Lin, T. -H. (2020). Customer online shopping feature extraction based on data mining algorithm. *International Journal of Smart Business and Technology*, 8(2), 41-50.

Cho, S. -S. & Choi, W. -H. (2020). Implementation of drowsiness detection and safe driving system. *International Journal of IT-based Public Health Management*, 7(1), 1-8. DOI:10.21742/IJIPHM.2020.7.1.01.

Cho, Y. -B. & Woo, S. -S. (2018). Automated ROI detection in left hand x-ray images using CNN and RNN. *International Journal of Grid and Distributed*

Computing, NADIA, ISSN: 2005-4262 (Print); 2207-6379 (Online), 11(7), 81-92. DOI: http://dx.doi.org/10.14257/ijgdc.2018.11.7.08.

Cui, Z. Shi, X., Chen, Y., & Guo, Y. (2016). A sense embedding of deep convolutional neural networks for sentiment classification. *International Journal of Grid and Distributed Computing*, NADIA, ISSN: 2005-4262 (Print); 2207-6379 (Online), 9(11), 71-80. DOI: http://dx.doi.org/10.14257/ijgdc.2016.9.11.06.

David, T. Johan, B., & Lin, C. (2021). Research on real-time data transmission between IoT gateway and cloud platform based on two-way communication technology. *International Journal of Smart Home*, 1(1), 61-74.

Divya Vani, R. (2015). Routing system with diversion in wireless ad hoc security. *Asia-pacific Journal of Convergent Research Interchange*, SoCoRI, ISSN: 2508-9080 (Print); 2671-5325 (Online), 1(4), 41-47, DOI: http://dx.doi.org /10. 21742/ APJCRI. 2015.12.06.

Golzarnia, A., Doostari, M. A., & Joghal, M. M. (2021). Secure registration of ATM cards on smartphones based on a secure mobile payment architecture consisting of the simcard and trustzone technology. *International Journal of Security and Its Applications*, NADIA, ISSN: 1738-9976 (Print); 2207-9629 (Online), 15(1), 35-44. DOI: http://dx. doi.or g/ 10.33832 /ijsia .2021.15.1.04.

Hinton, G. E., Salakhutdinov, R. R. (2006). Reducing the dimensionality of data with neural networks. *Science*, 313(5786), 504-507.

Ibor, A. E., Oladeji, F. A., & Okunoye, O. B. (2018). A survey of cyber security approaches for attack detection, prediction, and prevention. *International Journal of Security and Its Applications*, NADIA, ISSN: 1738-9976 (Print); 2207-9629 (Online), 12(4), 15-28. DOI: http://dx.doi.org /10.14257 /ijsia.2018 .12.4.02.

Jiang, R. (2016). Dimensionality reduction on anchorgraph with an efficient locality preserving projection. *Eurocomputing*, 187, 109-118.

Jung, C. Y. & Keerthana, V. B. (2015). A computational dynamic trust model for user authorization. *Asia-pacific Journal of Convergent Research Interchange*, SoCoRI, ISSN: 2508-9080 (Print); 2671-5325 (Online), 1(4), 1-6. DOI: http://dx.doi.org/10.21742/ APJCRI. 2015.12.01.

Kim, D. (2018). Deep learning neural networks for automatic vehicle incident detection. *Asia-pacific Journal of Convergent Research Interchange*, SoCoRI, ISSN: 2508-9080 (Print); 2671-5325 (Online), 4(3), 107-117. DOI: http://dx.doi.org/10.14257/apjcri.2018.09.11.

Kim, J. H. & Bhatele, K. R. (2016). Recognition using cyber bullying in view of semantic-enhanced minimized auto-encoder. *Asia-pacific Journal of Convergent Research Interchange*, SoCoRI, ISSN: 2508-9080 (Print); 2671-5325 (Online), 2(44), 7-14. DOI: http://dx.doi.org/ 10 .217 42/APJCRI.2016.12.02.

Kim, J. -H., Lee, S. -W., & Youn, J. -H. (2021). Malicious code characteristics visualization using API. *International Journal of Smart Home*, 1(1), 65-84.

Kim, H. K., Yeo, H., Kim, T. H., Ramos, C., Marreiros, G., & Hwang, H. J. (2016). Developmental approaches covering context area mobile applications service oriented architecture and model driven architecture. *International Journal of Future Generation Communication and Networking*, NADIA, ISSN: 2233-7857 (Print); 2207-9645 (Online), 9(12), 329-338. DOI: http:/ /dx.doi.org /10.1425 7/ijf gcn . 2016 .9.12.30.

Kim, T. -H. (2021). Electricity theft detection using fusion dense Net-RF model. *International Journal of Smart Home*, 1(1), 9-22.

Kim, T. -H. & Sakurai, K. (2008). Definition of security practices in security management part of security level management model. *International Journal of Security and Its Applications*, NADIA, ISSN: 1738-9976 (Print); 2207-9629 (Online), 2(1), 63-71.

Lee, C. -S. (2018). Security authentication technique using hash code in wireless RFID environments. *International Journal of Grid and Distributed Computing*, NADIA, ISSN: 2005-4262 (Print); 2207-6379 (Online), 11(10), 93-102. DOI: http://dx.doi.org/10.14257/ijgdc.2018.11.10.08.

Lee, J. Y. & Kolasani, L. (2015). Security based network for health care system. *Asia-pacific Journal of Convergent Research Interchange*, SoCoRI, ISSN: 2508-9080 (Print); 2671-5325 (Online), 1(1), 1-6. DOI: http://dx.doi.org/10.21742/APJCRI.2015.03.01.

Lee, Y. -K. & Park, D. -W. (2018). Design of internet of things business model with deep learning artificial intelligence. *International Journal of Grid and Distributed Computing*, NADIA, ISSN: 2005-4262 (Print); 2207-6379 (Online), 11(7), 11-22. DOI: http://dx.doi.org /10.14257/ijgdc .2018.11.7.02.

Li, L. (2019). An extensive review on recent deep learning applications. *Asia-pacific Journal of Convergent Research Interchange*, SoCoRI, ISSN: 2508-9080 (Print); 2671-5325 (Online), 5(3), 221-231. DOI: http://dx.doi.org/10.21742/apjcri.2019.09.22.

Li, W. (2011). Locality-preserving dimensionality reduction and classification for hyperspectral image analysis. *IEEE Trans Geosci Remote Sens*, 50(4), 1185-1198.

Madhavi, S. & Kim, T. H. (2021). Secured quantum wireless sensor network using IQOTP and super dense coding. *International Journal of Future Generation Communication and Networking*, NADIA, ISSN: 2233-7857 (Print); 2207-9645 (Online), 14(1), 59-74. DOI: http://dx.doi.org/10.33832/ijfgcn.2021.14.1.06.

Mandal, B. K., Bhattacharyya, D., & Kim, T. -H. (2014). A design approach for wireless communication security in bluetooth network. *International Journal of*

Security and Its Applications, NADIA, ISSN: 1738-9976 (Print); 2207-9629 (Online), 8(2), 341-352. DOI: http://dx.doi.org/10.14257/ijsia.2014.8.2.35.

Mandal, B. K., Bhattacharyya, D., & Kim, T. -H. (2014). An architecture design for wireless authentication security in bluetooth network. *International Journal of Security and Its Applications*, NADIA, ISSN: 1738-9976 (Print); 2207-9629 (Online), 8(3), 1-8. DOI: http://dx.doi.org/10.14257/ijsia.2014.8.3.01.

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security Privacy*, 16(5), 38-41.

Nadella, B. (2016). Data encryption using geometric range. *Asia-pacific Journal of Convergent Research Interchange*, SoCoRI, ISSN: 2508-9080 (Print); 2671-5325 (Online), 2(3), 21-28. DOI: http://dx.doi.org/10.21742/APJCRI.2016.09.03.

Nooribakhsh, M. & Mollamotalebi, M. (2018). A review on statistical approaches for anomaly detection in DDoS attacks. *International Journal of Security and Its Applications*, NADIA, ISSN: 1738-9976 (Print); 2207-9629 (Online), 12(6), 13-26. DOI: http://dx.doi.org/ 10.14257/ ijsia.2018.12.6.02.

Olson, C. C., Judd, K. P., Nichols, J. M. (2018). Manifold learning techniques for unsupervised anomaly detection. *Expert Syst Appl*, 91, 374-385.

Papernot, N., McDaniel, P. D., Wu, X., Jha, S., & Swami, A. (2015). Distillation as a defence to adversarial perturbations against deep neural networks [Online]. Available: https://arxiv.org/abs/1511.04508

Patil, S & Anandhi, R. J. (2021). Determining crime pattern based on clusters using guided population with dominancy supported genetic algorithm. *International Journal of Grid and Distributed Computing*, NADIA, ISSN: 2005-4262 (Print); 2207-6379 (Online), 14(1), 19-34. DOI: http://dx.doi.org/10.33832/ijgdc.2021.14.1.03.

Pullagujju, G. K. (2016). Identifying trojan facebook applications. *Asia-pacific Journal of Convergent Research Interchange*, SoCoRI, ISSN: 2508-9080 (Print); 2671-5325 (Online), 2(4), 1-6. DOI: http://dx.doi.org /10.21742/APJCRI.2016.12.01.

Rebentrost, P., Mohseni, M., & Lloyd, S., (2014), Quantum support vector machine for big data classification. *Physical Review Letters*, 113, 130503.

Rubinstein, B. I. P., Nelson, B., Huang, L., Joseph, A. D., Lau, S. -H., Rao, S., Taft, N., & Tygar, J. D. (2009). ANTIDOTE: Understanding and defending against poisoning of anomaly detectors. In Proc. ACM SIGCOMM Internet Measurement Conference.

Sarddar, D., Chakraborty, S., & Sen, P. (2017). Edge server selection in distributed content delivery network using k-means square classification algorithm and ant

colony optimization. *International Journal of Grid and Distributed Computing*, NADIA, ISSN: 2005-4262 (Print); 2207-6379 (Online), 10(9), 1-12. DOI: http://dx.doi.org/ 10.14257/ijgdc. 2017.10.9.01.

Schmidhuber, J. (2015). Deep learning in neural networks: An overview," *Neural Netw*, 61, 85-117.

Schuld, M., Bocharov, A., Svore, K. M., & Wiebe, N. (2020). Circuit-centric quantum classifiers." *Physical Review*, A 101.

Shin, S. M. & Uroosa, S. K. (2015). Predicting software reliability using particle swarm optimization technique. *Asia-pacific Journal of Convergent Research Interchange*, SoCoRI, ISSN: 2508-9080 (Print); 2671-5325 (Online), 1(3), 17-30. DOI: http://dx.doi.org/10.21742/APJCRI.2015.09.02.

Song, W. (2021). A new deep auto-encoder using multiscale reconstruction errors and weight update correlation. *Inf Sci*, 559, 130-152.

Song, Y. -j. & Lee, J. -K. (2020). Blockchain-based fog-enabled energy IoT architecture. *International Journal of Energy, Information and Communications*, 11(1), 23-30. DOI:10.21742/IJEIC.2020.11.1.04.

Son, Y., Oh, S., & Lee, Y. (2018), Hybrid deep neural network based performance estimation method for efficient offloading on IoT-cloud environments. *International Journal of Grid and Distributed Computing*, NADIA, ISSN: 2005-4262 (Print); 2207-6379 (Online), 11(7), 23-30. DOI: http://dx.doi.org/10.14257/ijgdc.2018.11.7.03.

Torlai, G. & Melko, R. G. (2020). Machine-learning quantum states in the NISQ era. *Annual Review of Condensed Matter Physics*, 11, 325-344.

Vaghela, K. (2020). E-commerce mobile payment risk trend prediction. *International Journal of Smart Business and Technology*, 8(2), 31-40.

Yeo, S. -S., Youk, S. -J., Park, G. -C., Kim, S. S., & Kim, T. -H. (2007). Physical threat description of smart card protection profile in security level 1st. *International Journal of Security and Its Applications*, NADIA, ISSN: 1738-9976 (Print); 2207-9629 (Online), 1(2), 99-104.