ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 10, No. 2, April 2022, pp.251-259

Deep learning model for cyber-attacks detection method in wireless sensor networks

Shaymaa Mahmood Naser[1], Yossra Hussain Ali[1], Dhiya Al-Jumeily OBE[2]
[1]Computer Science Department, University of Technology, Baghdad, Iraq
[2]Asscoicate Dean, Head of Enterprise, Faculty of Engineering and Technology, Liverpool John Moores University, UK

ABSTRACT

Nowadays, electronic applications are being adopted instead of many traditional processes in data and information management that use Internet technology as a transmission medium. Therefore, these data and information suffer from different types of attacks that aim to destroy or steal them. One of these attacks is the cyber classification that can halt the whole system. In this paper, a cyber-attacks detector method is proposed based on deep learning technology for Wireless Sensor Network (WSN). This method adopts the behavior of the WSN's nodes as well as the data transmission that depends on the MQTT protocol. The use of the deep learning model in this method improves the detection accuracy compared to traditional machine learning methods. The results demonstrate the efficiency of using the combination of deep learning CNN-LSTM techniques to be 96.02% in training accuracy and 95.08% for validation accuracy depending on the dataset of [1]. The machine learning model in [1] obtains an accuracy between 87% and 91% for the augmented dataset processes.

Keywords: Deep learning, Machine learning, CNN-LSTM, WSN.

Corresponding Author:

Dhiya Al-Jumeily
Associate Dean / Head of Enterprise, Faculty of Engineering and Technology
Liverpool John Moores University
Liverpool, UK
E-mail: D.Aljumeily@ljmu.ac.uk

1. Introduction

Artificial Intelligence (AI) is a broad phrase that refers to technologies' ability to accomplish activities performed by the human brain, such as recognizing images, reacting, and making decisions [2]. It is now employed in a variety of sectors, including medicine [3], engineering [4], military operations [5], economics [6], prediction control of complex systems [7], [8], security [9], etc. To protect computers, servers, information systems, networks, and data from attacks, the level of information security must be structured with the purposes of integrity, availability, and confidentiality, especially in WSNs. It is important to note that security, particularly cyber-security, in WSNs has been considered one of the biggest challenges today in the research scope. This is due to the limitation of resources that negatively reflects the need for efficient encryption and authentication schema with low complexity. Cyber-security plays a major role in protecting the framework from threats by adopting artificial intelligence techniques such as deep learning (DL) and machine learning (ML) to build a smart attack detection model. Artificial Intelligent models require specific cyber-security defense and protection solutions [10]- [12]. ML relies on the idea of learning from previous examples and experiences for classification or clustering, as it is used in several areas of cyber-security, including the detection of zero-day attacks, prediction systems, etc. ML methods are classified into supervised, unsupervised, semi-supervised, and reinforcement. ML is designed for stable environments resources. Therefore, cyber-security, built with ML, suffers from cyber-attacks with intelligent ability that can change the stability of the resources to be an unstable environment. [13], [14]. On the other hand, Deep learning (DL) is a subset of machine learning but with more complexity and efficiency. DL can be considered a set of algorithms in machine learning in multiple stages with a wide range of datasets used to train the presented algorithms. [15]. With the rise of cybercrime, cybersecurity is the most important part of government systems to protect t the exchanged and stored information and data

from attackers. The intelligence techniques, including deep and machine learning methods, are used in cyber-security [16], as they have proven their effectiveness in detecting attackers, intrusion, malware, and spam [17]. In this work, a DL based cyber-attacks detection method is proposed for WSN. The DL method is adopted to improve the detection accuracy compared to traditional methods, such as machine learning. Since the WSN has limited resources, it is necessary to detect attacks at an early stage in order to prevent the loss of available resources. The proposed method is tested over the dataset of [1], and the results are compared with the machine learning methods of [1]. Compared to ML methods, the detection accuracy is enhanced by 5-9% in DL.

2. Related work

Cyber-security has been discussed by many researchers that aimed at enhancing techniques of detecting attacks in WSNs. In [13], the researchers presented many machine learning techniques used in cyber-security applications. This was done to determine what kinds of attacks these algorithms are exposed to. These techniques could change the attackers to be ineffective that are simulated using SCADA system and intrusion detection for VANET. In [14], the main and sub-categories of machine learning were adopted in cyber-security to detect spam, phishing page, malware, DOS attack, and biometric identification. Six ML methods using MQTT protocol were proposed to classify attacks by simulating a novel dataset in [18]. These methods were Logistic Regression, Gaussian Nave Bayes, k-Nearest Neighbors, Support Vector Machine, Decision Trees and Random Forests techniques. The results were sufficient enough to perform attack classification. While in [1], the authors also presented another six ML methods, including Nave Bayes, Decision Trees, Random Forests, Neural Network, Gradient Boost and Multilayer Perception. They were applied to a novel dataset to protect IoT systems. The result proved that the proposed methods were performed efficiently in detecting the attacks. The authors of [19] used ML techniques of Random Forest, KNN classifier, and SVM on MQTT-dataset, but with more accuracy for detecting attacks on IoT networks. In [15] and [16], the researchers showed a survey for DL method, including deep auto-encoders, restricted Boltzmann machines, recurrent neural networks, generative adversarial networks, and several others for cyber-security applications. They presented the challenges faced by cyber-security to these techniques. The authors of [20] suggested a DL model to detect DDoS cyber-security attacks on CICIDS2017 datasets with an accuracy of up to 97.16%. These results were much more efficient in comparison to the traditional methods of ML over the same dataset.
In [21], a survey on confirmed and recent researches of deep learning in cyber-security since 2018 until now was presented. This means that today's modern trend is towards intelligence algorithms for deep learning.

3. Deep learning

As explained before, the DL method is one of the intelligent machine learning techniques. It deals with a huge amount of data, and this, in turn, can help to predict and prevent attacks in cyber-security issues [22]. Different methods of DL can be used in cyber-security, such as Deep Belief Networks (DBN), Recurrent Neural Network (RNN), Convolutional Neural Networks (CNN), Generative Adversarial Networks (GAN) and Recursive Neural Networks (RCNN). The CNN is used for recognition systems based on 1D, 2D, 3D arrays of data. This data includes spectrograms of audio, videos, volumetric images, etc. DL consists of convolution layers, pooling layers, and the classification layer [15]. In this work, the DL is adopted in two models that are explained below.

3.1. Convolutional neural networks model

Convolutional neural network, often known as ConvNet or CNN, is a deep neural network architecture as shown in Figure (1). It is designed to handle data with a predefined, grid-like topology, such as 1D, 2D or 3D data for images and audio signals and 4D data for videos. ConvNets have three main characteristics: Weight sharing, subsampling, and the local receptive field (pooling). Image classification, object detection, audio recognition, natural language processing, and medical image analysis are just a few of the domains in which ConvNets has excelled. ConvNet is the backbone of computer vision, which has a wide range of applications, including self-driving cars and robotics, as well as blindness cures [23].

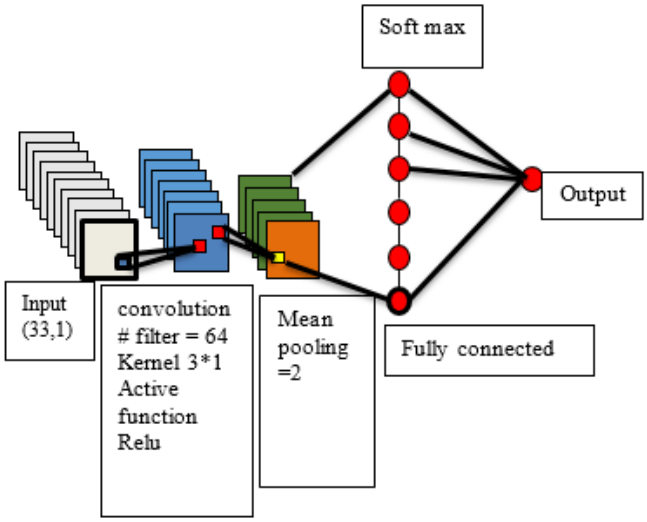

Figure 1. CNN Architecture

3.2. Long short-term memory model (LSTM)

It is built based on RNN technology to be the most popular RNN architecture to date as shown in Figure (2). LSTM eliminates the vanishing gradient problem in RNN as a result of its complex architecture. LSTM is different from RNN architecture and designed to work on long-term dependencies in data. LSTM is proved to be effective in speech recognition tasks where special memory cells of LSTMs are used to identify long dependencies [23], [24].

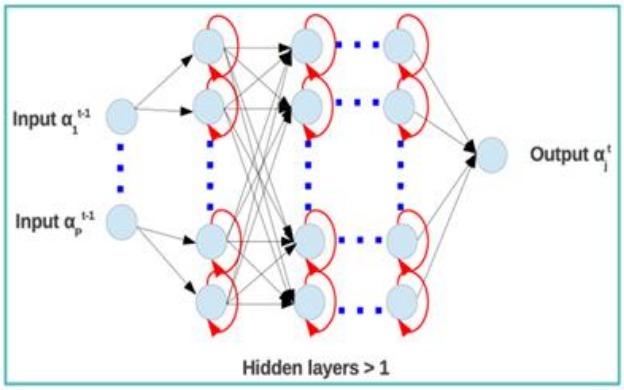

Figure 2. LSTM structure [24]

4. Proposed cyber-attack detection method

The deep learning technique is adopted in designing the proposed cyber-attack method to perform smart behavior. In order to focus on the essential details in the proposed method, this section is divided into two sub-sections.

4.1. Proposed method design

The proposed method is designed based on hybrid CNN and LSTM deep learning techniques. This is to classify the types of attacks that appeared in the adopted MQTT2020 dataset as presented in [1].
It should be highlighted that the utmost contribution of this work is to propose a hybrid deep learning model involving two neural network layers: CNN and LSTM. This hybrid model produces higher predictive performance when compared to the traditional deep learning models of CNN or LSTM alone.
Figure (3) shows the CNN-LSTM model, in which features are selected and then fed to the illustrated architecture. The first convolution with the kernel is built in dimensions of (3 x 1 x 128) and bias 128 used ReLU function. The second convolution with the kernel is built in dimensions of (3 x 128 x 128) and bias 128. The output of the stage so far is fed to the Maxpooling layer 1D. Finally, the third and fourth convolution layers are built in dimensions of (3 x 128 x 64), and (3 x 64 x 32), respectively, with bias 64 and 32. The output matrix

contains weights obtained through LSTM layer with dimensions of (32 x 128) using Tanh function. The batch normalization is applied with gamma of 32, beta of 32, moving mean of 32 and moving variance of 32. The design is ended by Dropout with fully connected 6 with 1x1.

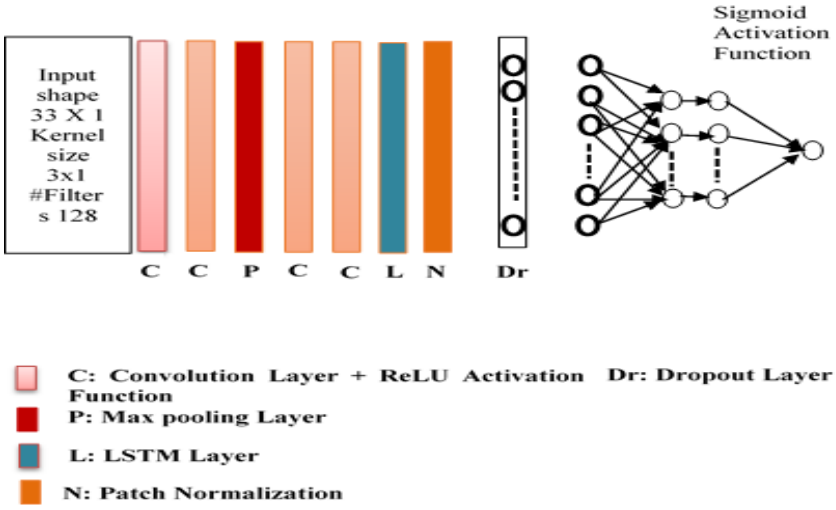

Figure 3. CNN- LSTM Model

4.2. The proposed algorithm

The presented cyber-attack detection method is performed based on the proposed algorithm shown in Figure (4) as a flowchart.

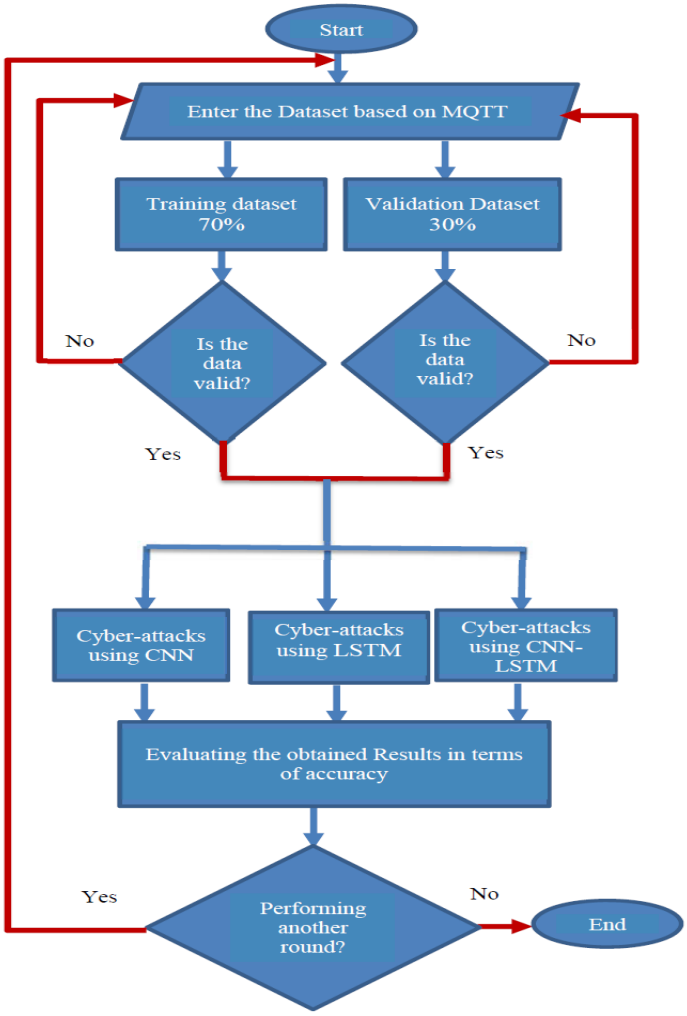

Figure 4. Algorithm Flowchart

The working steps of the proposed algorithm have been summarized as follows:

1. The dataset is entered into the algorithm.
2. The dataset is divided into training with 70% of data and validation with 30% of data.
3. These sets of data are checked whether they are valid or not. In case they are valid, the datasets are fed to the designed CNN_LSTM method for training and checking the validity. Otherwise, the dataset is fed again to the algorithm.
4. The designed CNN_LSTM performs the training and validation on the entered datasets and obtains the results.
5. The results are divided into CNN based, LSTM based, and CNN_LSTM based methods.
6. The results are evaluated by evaluating the accuracy.
7. The algorithm can be repeated or ended depending on the requirements.

4.3. Dataset

The adopted dataset for detecting the cyber-attacks in WSN is taken from [1]. This dataset includes different factor readings from the MQQT breaker simulation software. It also contains the data that suffers from different types of cyber-attacks that affect the values of normal information exchange inside the WSN. Table 1 illustrates the included factors adopted as features to be fed to the proposed CNN-LSTM based deep learning cyber-attack detection method.

Table 1. The features of dataset [1]

No	Name	Description	Protocol Layer
1	tcp.flags	TCP flags	TCP
2	tcp.time_delta	Time TCP stream	TCP
3	tcp.len	TCP Segment Len	TCP
4	mqtt.conack.flags	Acknowledge Flags	MQTT
5	mqtt.conack.flags.reserved	Reserved	MQTT
6	mqtt.conack.flags.sp	Session Present	MQTT
7	mqtt.conack.val	Return Code	MQTT
8	mqtt.conflag.cleansess	Clean Session Flag	MQTT
9	mqtt.conflag.passwd	Password Flag	MQTT
10	mqtt.conflag.qos	QoS Level	MQTT
11	mqtt.conflag.reserved	(Reserved)	MQTT
12	mqtt.conflag.retain	Will Retain	MQTT
13	mqtt.conflag.uname	User Name Flag	MQTT
14	mqtt.conflag.willflag	Will Flag	MQTT
15	mqtt.conflags	Connect Flags	MQTT
16	mqtt.dupflag	DUP Flag	MQTT
17	mqtt.hdrflags	Header Flags	MQTT
18	mqtt.kalive	Keep Alive	MQTT
19	mqtt.len	Msg Len	MQTT
20	mqtt.msg	Message	MQTT
21	mqtt.msgid	Message Identifier	MQTT
22	mqtt.msgtype	Message Type	MQTT
23	mqtt.proto_len	Protocol Name Length	MQTT
24	mqtt.protoname	Protocol Name	MQTT
25	mqtt.qos	QoS Level	MQTT
26	mqtt.retain	Retain	MQTT
27	mqtt.sub.qos	Requested QoS	MQTT
28	mqtt.suback.qos	Granted QoS	MQTT
29	mqtt.ver	Version	MQTT
30	mqtt.willmsg	Will Message	MQTT
31	mqtt.willmsg_len	Will Message Length	MQTT
32	mqtt.willtopic	Will Topic	MQTT
33	mqtt.willtopic_len	Will Topic Length	MQTT

5. Results

In order to test the proposed method of detecting the cyber-attacks in WSN, the augmented MQTT-dataset2020 of [1] is adopted and the results obtained from [1] are compared with the achieved results of the proposed method. The MQTT protocol is adopted to obtain the results, and MQTT breaker for monitoring the WSN performance. The augmented dataset represents the real-time data without any reduction applied in [1] according to the requirements of the presented ML models. Therefore, the augmented dataset includes huge data records reflected positively on the training and validation stages in DL methods. The simulator adopts the Python programming language that depends on object-oriented programming and effectively integrates with systems. The framework of Keras with TensorFlow engine [25] is used in designing the proposed method. The approved experiences in defense and security applications were also taken into consideration in [26]-[31]. In Figure (5), the accuracy performance over the used epochs for the proposed CNN-LSTM method is drawn. While Figure (6) shows the loss in the proposed method that varies with epochs. It is concluded that the variation in both figures in terms of accuracy and loss is limited to 1% in accuracy and 0.05% in loss. Therefore, there is no need for increasing the number of epochs.

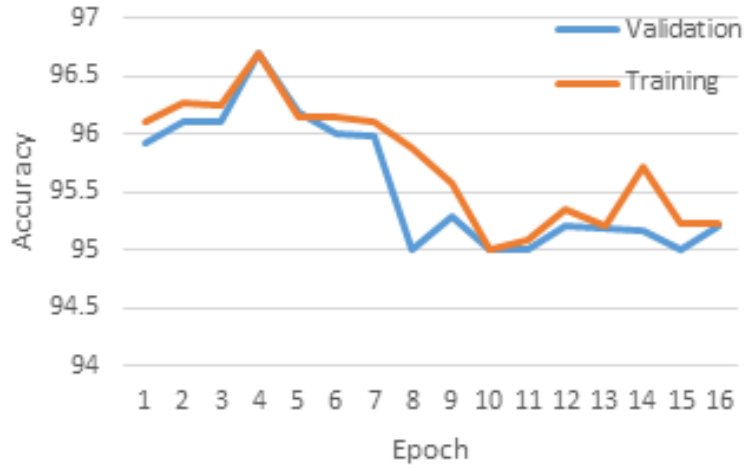

Figure 5. The accuracy vs. epochs for the proposed method

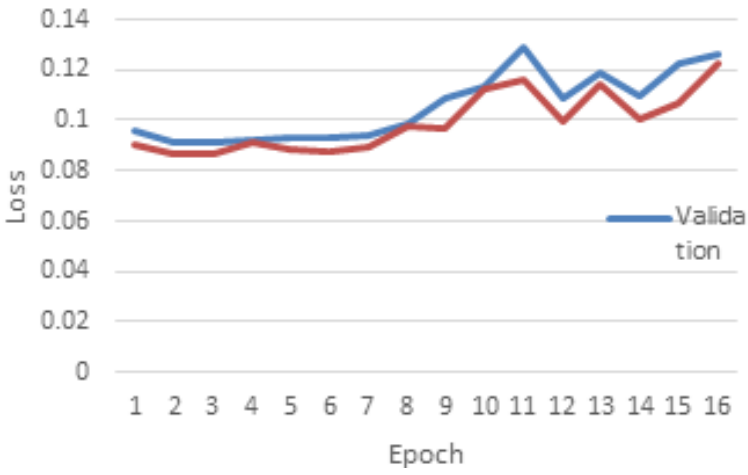

Figure 6. The loss vs. epochs for the proposed method

Table 2 explains the achieved results of the proposed method as well as the ML based auto-encoder method. From this table, it is clearly evident that the proposed cyber-attack detection based on the combination of CNN-LSTM methods improves the calculated accuracy for both training and validation by (5-9%). The range of accuracy with ML methods in [1] was 87-91%, whilst in the proposed method CNN_LSTM was 95-96%. These

are the results of the ability of deep learning methods considering the big data (millions) in the dataset, while the ML methods suffer from overfitting and delay in running. In WSN, the delay is prohibited due to the limited resources of power. Although the DL methods need more execution time in training in comparison with the ML methods, it needs this time once at the training and the real-time run is kept in a low level of processing with high accuracy in detecting the attacks.

Table 2. Accuracy results of DL and ML methods

Techniques	MQTT2020 Dataset	
	Training Accuracy	Validation Accuracy
CNN with augmented-dataset	88%	87%
LSTM with augmented-dataset	79%	77%
CNN-LSTM with augmented-dataset	96.7%	96.7%
ML-Different methods with augmented-dataset [1]	87-91%	87-91%

On the other hand, Figure (7) shows the confusion matrix that is used in performing the compared methods.

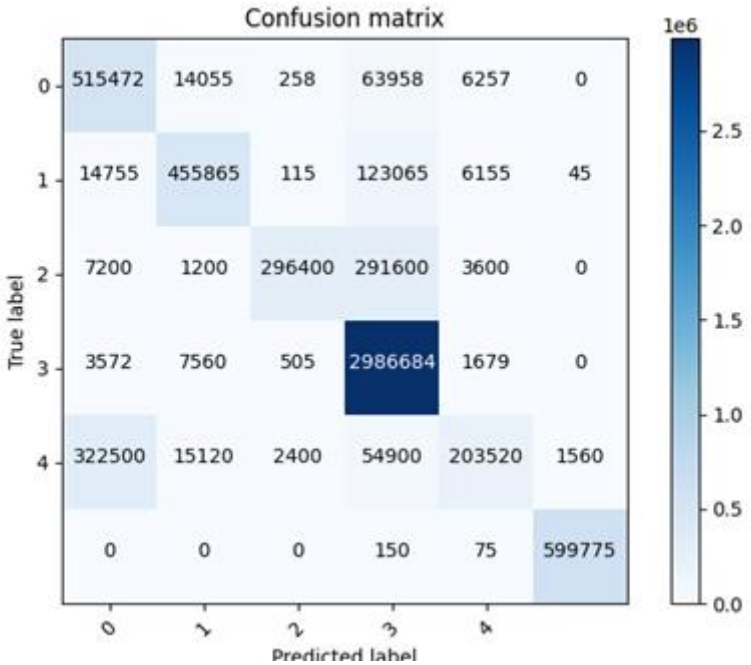

Figure 7. The confusion matrix for the proposed method

6. Conclusion

A cyber-security method for detecting the attacks was proposed based on the combination of DL methods of CNN and LSTM. The DL-CNN_LSTM techniques were used to improve the performance of the proposed detection method in terms of accuracy for both training and validation. The MQTT protocol was adopted, and the MQTT-dataset2020 presented in [1] was considered in testing the proposed method. The results showed that the combination of CNN and LSTM methods enhanced the accuracy of detection and classification of cyber-attacks to reach 96% for training and 95% for validation. According to these ratios, the proposed methods outperformed the traditional methods of ML.

References

[1] I. Vaccari, G. Chiola, M. Aiello, M. Mongelli, and E. Cambiaso, "MQTTset, a New Dataset for Machine Learning Techniques on MQTT", *Sensors*, MDPI, 18 Novmber 2020.

[2] A. Mellita, and S. A. Kalogirou, "Artificial intelligence techniques for photovoltaic applications: A review", *Progress in Energy and Combustion Science34*, p. 574–632, Elsevier, 4 January 2008.

[3] F. Shi, J. Wang, J. Shi, Ziyan Wu, Qian Wang, Zhenyu Tang, Kelei He, Yinghuan Shi; Dinggang Shen,"Review of Artificial Intelligence Techniques in Imaging Data Acquisition, Segmentation, and Diagnosis for COVID-19", *IEEE Reviews in Biomedical Engineering*, Volume 14, 16 April 2020.

[4] I. K. Nti, A. Adekoya, B. Weyori, and O. Nyarko-Boateng, "Applications of artificial intelligence in engineering and manufacturing: a systematic review", *Journal of Intelligent Manufacturing*, 2021.

[5] P. Svenmarck, L. Luotsinen, M. Nilsson, and J. Schubert, "Possibilities and Challenges for Artificial Intelligence in Military Applications", *Conference: NATO Big Data and Artificial Intelligence for Military Decision Making Specialists*, Project AI for decision support and cognitive systems, May 2018.

[6] C.-HuiLu, "The impact of artificial intelligence on economic growth and welfare", *Journal of Macroeconomics***,** Vol. 69, September 2021.

[7] A. Kaab, M. Sharifi, H. Mobli, A. Nabavi-Pelesaraei, and K.-wing Chau, "Combined life cycle assessment and artificial intelligence for prediction of output energy and environmental impacts of sugarcane production", *Science of the Total Environment*, Elsevier, pp 1005-1019, 2019.

[8] Y. Mohamadou, A. Halidou, and P. T. Kapen, "A review of mathematical modeling, artificial intelligence and datasets used in the study, prediction and management of COVID-19", *Applied Intelligence*, part of Springer Nature 2020, 06 July 2020.

[9] D. S. Hoadley, and N. J. Lucas," Artificial Intelligence and National Security", congressional research service ,26 April 2018.

[10] K. CHELLI, "Security Issues in Wireless Sensor Networks: Attacks and Countermeasures", *Proceedings of the World Congress on Engineering 2015*, Vol I, London, U.K., July 2015.

[11] D. He, S. Chan, and Mohsen Guizani, "Cyber Security Analysis and Protection of Wireless Sensor Networks for Smart Grid Monitoring", *IEEE Wireless Communications*, 2016.

[12] Jian-hua LI, "Cyber security meets artificial intelligence: a survey", *Frontiers of Information Technology & Electronic Engineering*, pp. 1462-1474, 2018.

[13] A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review", *WIREs Data Mining Knowl Discovry*, Wiley, 2019.

[14] T. Thomas, A. P. Vijayaraghavan, and S. Emmanuel, "Machine Learning Approaches in Cyber Security Analytics", eBook, *Springer Nature Singapore*, 2020.

[15] D. S. Berman, A. L. Buczak, J. S. Chavis, and Cherita L. Corbett, "A Survey of Deep Learning Methods for Cyber Security", *information journal*, MDPI, 02 April 2019.

[16] N. R. Reddy Gade, and U. G. Reddy," A Study of Cyber Security Challenges and its Emerging Trends on Latest Technologies", *arXiv*, Springer, Feb 2014.

[17] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, "On the Effectiveness of Machine and Deep Learning for Cyber Security", *Conference: 2018 10th International Conference on Cyber Conflict (CyCon)*, May 2018.

[18] H. Hindy, M. Bures, C. Tachtatzis, and X. Bellekens, "Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study", *arXiv*, Springer, June 2020.

[19] J. Makhija A. Appu Shetty, and A. Bangera, "Classification of Attacks on MQTT-Based IoT System Using Machine Learning Techniques", *Part of the Advances in Intelligent Systems and Computing book series*, vol. 1394, 29 Augest 2021.

[20] M. Roopak, G. Yun Tian, and J. Chambers, "Deep Learning Models for Cyber Security in IoT Networks", *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, January 2019.

[21] M. Amine Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection Approaches,dataset compartive study", *Journal of Information Security and Applications*, ELSEVIER, 2019.

[22] P. Dixit, and S. Silakari, "Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review", *Computer Science Review*, ELSEVIER,2020.

[23] M. Arif Wani, F. A. Bhat, S. Afzal, and A. Khan, “Advances in Deep Learning”, Studies in Big Data, Springer, vol. 57, 2020.

[24] A. Shewalkar, D. Nyavanandi, and S. A. Ludwig, “Performance Evaluation of Deep Neural Networks Applied to Speech Recognition: RNN, LSTM AND GRU”, *JAISCR*, vol. 9, No. 4, pp.235-245, 10 March 2019.

[25] F. Chollet, “Deep Learning with Python”, Manning Publications Co, 2018.

[26] H. Salim, and H. Tauma, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 16, pp. 144-157, 2021.

[27] H. ALRikabi, and A. Ibtisam A. Aljazaery, "Encryption of Color Image Based on DNA Strand and Exponential Factor," *International journal of online and biomedical engineering(iJOE)*, vol. 18, no. 3, 2022.

[28] H. Tauma, N. Alseelawi, and H. TH. "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT," *International journal of online and biomedical engineering*, vol. 18, no. 3, 2022.

[29] H. T. Salim, N. A. Jasim, "Design and Implementation of Smart City Applications Based on the Internet of Things," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 15, no. 13, pp. 4-15, 2021.

[30] I. A. Aljazaery, and M. R. Aziz, "Combination of Hiding and Encryption for Data Security," *International Journal of Interactive Mobile Technologies*, vol. 14, no. 9, pp. 34-47, 2020.

[31] R. A. Azeez, M. K. Abdul-Hussein, and M. S. Mahdi, "Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique," *Periodicals of Engineering Natural Sciences*, vol. 10, no. 1, pp. 178-187, 2022.