


A Novel Cyber-attack Leads Prediction System using Cascaded R2CNN Model

P. Shanmuga Prabha¹ 

Assistant Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamilnadu, India, Pincode: 602105

S. Magesh Kumar² 

Professor, Department of Computer Science and Engineering Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University Chennai, Tamilnadu, India, Pincode: 602105

Abstract—Novel prediction systems are required in almost all internet-connected platforms to safeguard the user information to get hacked by intermediate peoples. Finding the real impacted factors associated with the Cyber-attack probes are being considered for research. The proposed methodology is derived from various literature studies that motivated to find the unique prediction model that shows improved accuracy and performance. The proposed model is represented as R2CNN that acts as the cascaded combination of Gradient boosted regression detector with recurrent convolution neural network for pattern prediction. The given input data is the collection of various applications engaged with the wireless sensor nodes in a smart city. Each user connected with a certain number of applications that access the authorization of the device owner. The dataset comprises device information, the number of connectivity, device type, simulation time, connectivity duration, etc. The proposed R2CNN extracts the features of the dataset and forms a feature mapping that related to the parameter being focused on. The features are tested for correlation with the trained dataset and evaluate the early prediction of Cyber-attacks in the massive connected IoT devices.

Keywords—Cyber security in smart devices; cyber security; cyber-attacks; internet of things; IoT devices; machine learning; wireless sensor networks

I. INTRODUCTION

In the current fast growing world, the demand on cyber security to users and IOT devices becomes mandatory due to the equivalent increase of cyber-attacks. The awesome growth of internet and networking models enables the users to get access the internet hassle free with flexible applications. Numerous cyber-attacks are predicted by the software and intrusion detection systems installed in the IOT devices and user accessible devices. Some of the frequently occurring cyber-attacks are denial-of-service(DoS) issue, software malwares, hacking due to unauthorized access, man in middle problem etc. the data industry get affected a lot due to the loss of secretive information that should be maintained [1].

Cyber security system is comprises of layers of protection starting from the physical layer to the application layer. Normally application layer resemble the end user connected with the certain network. Physical layer security plays a vital role in holding the data and making the secure communication with the data link layer. Nowadays in most of the systems, a powerful intrusion detection model is developed and installed.

These detectors filter out the malwares to some extent. Working on achieving accurate intrusion detection systems are also focused by research team. The author in [1] discussed recently with intrusion detection system using tree method that is named as intruDTree that keeps the decision tree as base model. The implemented intruDTree creates various test cases and expressions to check the real impact of the action takes place in to the IOT device. [2]Evaluated a signature based approach in the development of intrusion detection system and intrusion prevention system. The malicious software damages the protection systems, in the form of worms that uses the same protocol to carry over the network. Machine learning based signature model is evaluated to adopt the changing frameworks and authenticate the new user every time. The level of authentication happens in each stages of network connectivity [3].

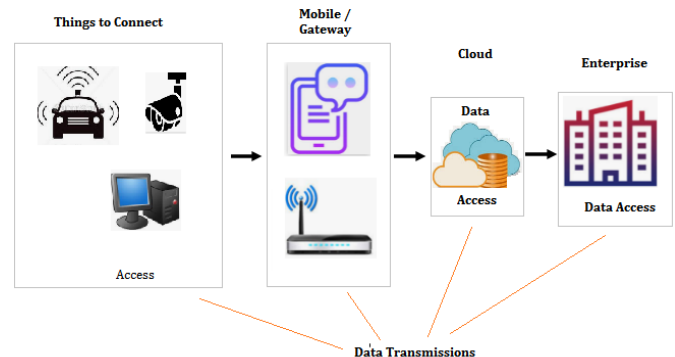


Fig. 1. Model of Cyber Security in IoT Devices.

Fig. 1 shows the architecture of cyber security framework. The model is explained in three phases. The first one is the data gathering phase in which the information in the form of images, videos, accessibility, unique codes, vehicle data and emergency information are collected. The second phase is the gateway or communication medium where the mobile gateway, data processing modules, android devices or wireless modems are connected. The cloud based accessibility also comes under the same category. The third phase is the application model in which the data is applied to the utilization of operations and control [4]. IoT based Cyber security monitoring for Internet dependent drones that gathers the tracking data and input patterns. Based on the available data, using Naïve Bayes model the system is able to identify

the cyber threats [4], further by addressing the existing issue of assumptions on information received need to be improving by utilization of better algorithms. Cyber security attacks get injected into the system once and consequences made by the attack exist for a long period. Cyber security system is needed in every single process associated with the organization [5].

The presented paper addresses the problem of resilient detection of threat and more processing time in the network. It also considers the major issue of system replay issues. The overtake of cyber threat dominates the system operation. The presented paper discusses the detailed Literature background in Section II. Followed by Section III, discuss the tool selection and impacts of specific tool to deep analysis of the proposed idea. Section IV. Discuss the design methodology of the proposed model, followed by Section V. Results and discussions are made.

II. LITERATURE SURVEY

K. Thakur et al., [6] discussed various cyber security threats in the form of data utilized, work enforcement, and protocols used to protect the user information. Emails and virus scanning assistance providing significant results are discussed. He investigated the peer review of papers with similar ideologies and found out the need for password protection frameworks in cyber security systems. The paper provides the knowledge on basic techniques to safeguard the IOT devices.

H. Bannasar et al., [7] evaluated a journal addressing various network security algorithms utilized for the cloud security threats. They discussed on cloud network model and its infrastructure that can be optimized. The cloud services such as SaaS, PaaS, IaaS being discussed and various threats such as data loss, Account hacking, malwares in the network and device malfunction etc.

R. Das et al., [8] discussed a journal stating various machine learning algorithms that incorporated with the development of cyber security models. A detailed survey has been framed and the comparative performance on each algorithm in terms of accuracy and error rate is evaluated. OneR algorithm, Naïve Bayes, random forest algorithms are discussed together to find the better performing model. Artificial neural network models and clustering algorithms are reviewed.

I. Duic et al., [9] highlighted the international cyber security standards in their research work stating the cyberspace implications in the global scenario. The paper explained much about the security risk and challenges to be expected in fast growing internet world. They elaborated the implementation as two phases. In the first phase they discussed about the summarized list of attacks that target the IOT devices. The second phase of discussion is about the intrusions present in the network. Throughout the paper information related to malwares, denial of service, unauthorized access and many key impacted factors are discussed.

D. Ratasich et al., [10] evaluated a research work that discusses the state of art approach of various existing cyber

security methodology on fault detection process, self-healing methodology and anomaly detection systems that is behind the resilience of cyber security devices. The amount of robustness is considered as one of the main attribute of sustaining the resilient issue in cyber security systems.

M. Saharkhizan et al., [11] evaluated a deep recurrent neural network model for detecting the cyber-attacks in internet controlled devices using traffic data of network. Deep LSTM model is associated with the ensemble detectors, to get the effective outcome on malware detection and achieved a rate of 99% of accuracy. The developed model is also tested with the Modbus data of network traffic. The correlated patterns helpful for us to determine the factors related with the cyber-attacks.

A. Sivanathan et al., [12] developed a challenging network classification model that is pre-trained by historical data streams of IoT traffics. They developed a one stop customized behavioral model for detecting the network performance. Automatic noise filtering is done before evaluating the traffic path. IOT devices connected with the certain traffic are intended to provide the demonstration on their individual performance.

Na Liu et al., [13] evaluated new perceptions on cyber-attacks over connected vehicles and autonomous vehicles. The research aimed to provide information on lack of knowledge on analyzing the cyber-attacks in user authentications, licensing part of CAV (connected and autonomous vehicles). Safety, awareness, responsibility education and trust factors are considered.

Isabel Arend et al., [14] they reported a detailed analysis on malwares and its attacks, to the cybercrimes feasibilities happening because of the lack of user security. The study reveals active risk and passive risk on cyber security behaviors. They concurrently evaluate the difference between the two risks present in the cyber security systems. The research underwent various challenges towards the discussions on theoretical and practical implications.

A. Related Work

Wang et al., [15] Apart from firewall security, conventional security systems are required for Supervisory control and Data acquisition (SCADA) is discussed in which deep learning approach is evaluated. It detects the malicious attacks in the SCADA environment and investigates the protection criteria of cyber-attacks detection process. Alkahtani et al., [16] Botnet attacks are one of the serious problems in cyber systems, which threatened the motion-less IoT devices. Empirical research was made on the malicious pattern detection using Convolution neural network (CNN) combined with Long-Short term memory Neural network (LSTM). It has the improved ability to detect the BOTNET attacks, with accuracy of 90.88%. F. Hossain et al., [17] a reliable cyber-attack detection model with ensemble classification model is evaluated. Gradient boost algorithm and random forest algorithm is converged for effective detection [18]. The static test and evaluation of cyber threat detection using LASSO classifier achieved the accuracy of 99% maximum [19].

III. SYSTEM DESIGN

The major addressable issue of Cyber security attacks in publicly available networks is the resilient response of the system for the injected issues, and those remains in the system for prolonged duration and permanently damages the organization credentials. The overall processing delay on attack detection and system replay issues are addressed here.

The novel cyber-attacks detection protocol is developed using the hybrid combination of cascaded R2CNN in which the regression analysis is cascaded in decision making with the recurrent convolution neural network model. The system design is implemented using MATLAB IDE by utilizing the regression tools and deep neural network toolbox. The system prediction model is developed in a recurrent fashion to test the weightage and apply the bias result again with the inputs that adapt the values.

IV. DESIGN METHODOLOGY

A. Design Summary

Fig. 2 shows the architecture of R2CNN cascaded model. The preprocessing part of the system uses adaptive principle component analysis and Singular value decomposition model combined to process the raw data. The LYSIS dataset consists of eight columns of received data. The dataset holds the parameters of connected device in the IOT modems. The feature mapped variables are applied to gradient boosted regression model in which the unsupervised analysis is made. The closely related parameters are plotted in regression plots as shown in Fig. 4(a) (b) and (c). The prediction result is based on two decisions. The decision one is created using the regression method.

Followed by regression cascaded fashion of recurrent Convolution neural network (R2CNN) is implemented. The dataset patterns after the feature mappings form a feature vectors. These vectors are resized to constant matrix dimension and fetched to RCNN model. R2CNN model consists of Input layer of size [100x1], max pooling layer, convolution layer (1x10: Stride) and fully connected layer (384x5 layers). The data is pattern compared at each stages of recurrent neural network.

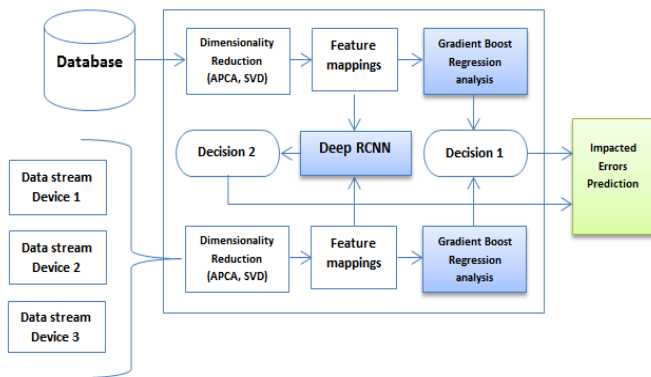


Fig. 2. Architecture Diagram of Cascaded R2CNN Prediction Model.

The loop of recurrence is varied for improving the performance. Every stage of analysis the weighted bias of the comparative result is updated. The profound R2CNN network is executed to distinguish the example coordinate between the data base and the test contribution of the IOT information. These examination results are additionally put away as large information stockpiling focuses for future analysis. The proposed framework utilizes four unique calculations and its similar outcomes.

The exactness of the forecast framework is determined utilizing the disarray network delivered toward the finish of R2CNN simulation. In case of threat pattern that does not correlate with any of the database learned patterns, then it is considered as the new threat and it is intended for learning purpose. Further new entries of cyber-attack patterns are also considered here. The disarray framework creates the boundaries, for example, Truepositive rate (TP), True negative rate (TN), false positive rate (FP) and False negative rate (FN). The exactness is determined utilizing the equation given in equation(1).

$$\text{Accuracy} = \frac{TN+TP}{TN+TP+FN+FP} \quad (1)$$

V. RESULT AND DISCUSSION

Fig. 3 shows the accuracy graph of deep R2CNN model that depicts the improved accuracy with respect to the increase in iteration of the analysis. The pre-trained data compared with the test input pattern from the device. In case of maximum correlation with the malware data in the database, the prediction system provides the label as output showing malware detection as message box showing the impacted factor such as prolonged duration, malicious application found or unauthorized notifications found, etc. as shown in Fig. 5.

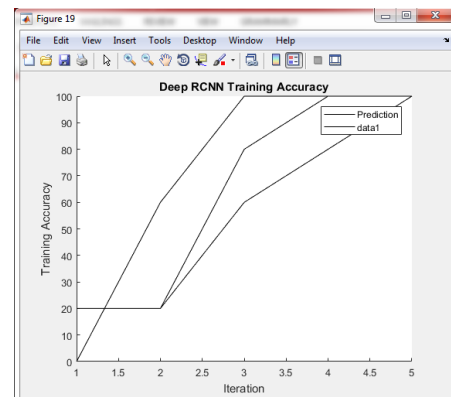


Fig. 3. Training Accuracy of Cascaded R2CNN.

Fig. 4 shows the regression analysis graph of direct method applied to the input data, 4(b) shows the regression analysis plot using Matlab inbuilt function, and 4(c) shows the regression analysis plot using gradient descent boosted regression method as proposed. The result of the regression model shows the maximum relative values towards the diagonal line. The regression result is considered as the decision 1 for final prediction. The detailed algorithm steps are shown.

Algorithm: Cascaded R2CNN

- 1 Get input data
- 2 Extract Features $X=features(data)$
- 3 Compute Gradient Descent Regression(X);
- 4 Fetch to RCNN model and store Result = weightage
- 5 Check bias (Result)& apply to Y
- 6 Repeat loop
- 7 Compare X and Y for max(Match score)
- 8 Call parameters(max(match_data))
- 9 Display parameters $p1,p2,p3$
- 10 Repeat all steps.

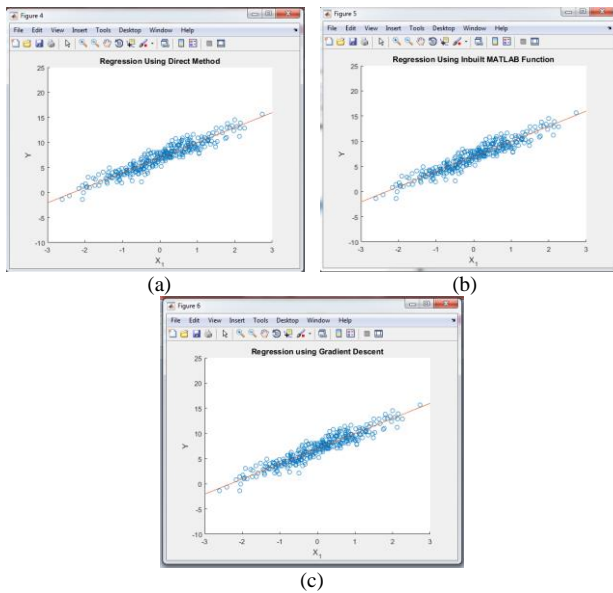


Fig. 4. (a) Regression Graph using Direct Method (b) Regression using Inbuilt Matlab Function (c) Regression using Gradient Descent Boosted Method.

Table I shows the Comparison results of Existing works and Proposed Cascaded R2CNN architecture. The author in [11] developed Cyber Threat detection in Traffic data using LSTM algorithm and achieved the accuracy of 99%. In [16], developed a LSTM with CNN configuration and achieved the accuracy of 90.88%. In [17], the author discusses the Massive cyber Protection system with Gradient Boost algorithms and Random forest models. Accuracy of 99% is achieved by the author. These studies helpful in deriving the proposed Cascaded architecture that combine the regression results as well as Convolution operation.

TABLE I. COMPARISON OF EXISTING WORK AND PROPOSED CR2CNN

S No	References	Concept	Algorithm	Accuracy
1	M. Saharkhizan et al., [11]	Cyber Threats detection in traffic data	LSTM	99%
2	Alkahtani et al., [16]	Cyber threat detection in SCADA	LSTM-CNN	90.88%
3	F. Hossain et al., [17]	Massive cyber system protection	GBR-RF	99%
4	Proposed Work	Cyber threat detection in Smart city Dataset- LYSIS	CR2CNN	99.2%

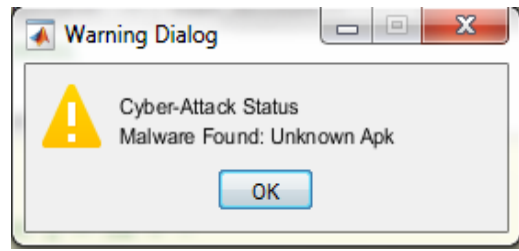


Fig. 5. Alert Notification.

Fig. 5 shows the Cyber-attack status after testing the input. The output also shows the parameter that impacted for malware. Example the above alert message displays the unknown APK found as parametric result that leads to cyber-attacks. The proposed algorithm focused on detecting the type of cyber-attack in short span of time. The resilience issue addressed is reduced here; comparatively the proposed system achieved the delay of 10.77 seconds.

Fig. 6 shows the mean square error of the three methods of regression analysis. From the above figure it is clear that gradient descent boosted model provides less error rate.

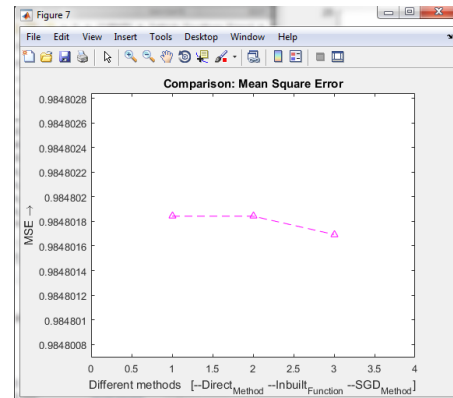


Fig. 6. Mean Square Error of Proposed Method.

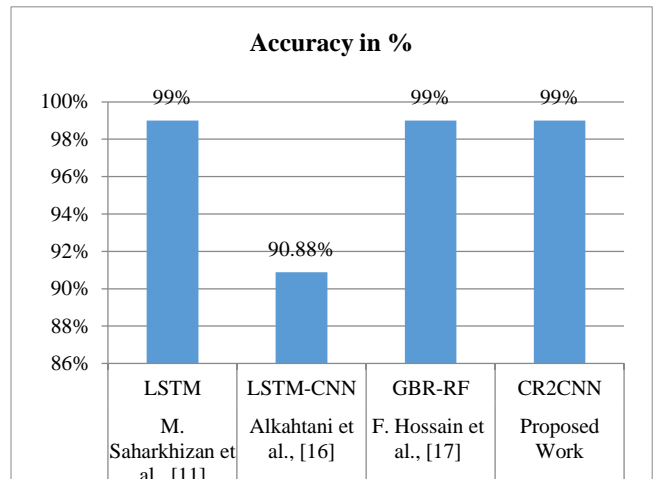


Fig. 7. Comparative Accuracy of Existing and Proposed Cyber-attack Detection Models.

Fig. 7 shows the comparison results of accuracy with various existing implementations. Considering the static dataset of LYSIS smart city, the presented system derives

maximum focus on reducing the processing delay for earliest prediction. The Cascaded R2CNN stands in the benefit of less computation steps. The stacked operation ensures the results with high confidence. Accuracy is high for the static approach anyway the present research need to be extended with dynamic approach on few real time threats in massive cyber physical systems. The proposed model tests the reliable communication in small enterprise level. Dynamic approach obviously extended for global discussion.

VI. CONCLUSION

Cyber-attack tracking and prevention is mandatory in almost every internet connected platforms. As an initiative the proposed system is focused on deriving a novel methodology to detect the most impacted leads for cyber-attacks in IoT networks. The proposed system consists of Novel algorithm named Cascaded R2CNN. Provided with LYSIS dataset, the developed model detects the Cyber threatening patterns. The addressed issue of early prediction is given priority here. The system achieved the early prediction of Cyber-attack patterns within 10.77 seconds. The proposed prediction model achieves 99.2% accuracy towards the given input dataset. Further the system modeled here is reliable for static testing of IoT networks in enterprise level. The proposed research work needs to be extended to achieve dynamic results by considering multiple environments and different patterns of Cyber-Threatening patterns.

REFERENCES

- [1] Sarker, I.H.; Abushark, Y.B.; Alsolami, F.; Khan, A.I. IntraDTree: A Machine Learning Based Cyber Security Intrusion Detection Model. *Symmetry* 2020, 12, 754.
- [2] R. Kozik and Michał Choraś "Machine Learning Techniques for Cyber Attacks Detection", published Springer international year 2014.
- [3] Aman, W. and Shukaili, J., 2021. A Classification of Essential Factors for the Development and Implementation of Cyber Security Strategy in Public Sector Organizations. *International Journal of Advanced Computer Science and Applications*, 12(8).
- [4] Majeed, R., Abdullah, N. and Mushtaq, M., 2021. IoT-based Cyber-security of Drones using the Naïve Bayes Algorithm. *International Journal of Advanced Computer Science and Applications*, 12(7).
- [5] Latifa Alzahrani, "Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes" *International Journal of Advanced Computer Science and Applications (IJACSA)*, 12(11), 2021. <http://dx.doi.org/10.14569/IJACSA.2021.0121172>.
- [6] K. Thakur, M. Qiu, K. Gai and M. L. Ali, "An Investigation on Cyber Security Threats and Security Models," 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, 2015, pp. 307-311, doi: 10.1109/CSCloud.2015.71.
- [7] H. Bannasar, M. Essaaidi, A. Bendahmane and J. Ben-othman, "State-of-the-art of cloud computing cyber-security," 2015 Third World Conference on Complex Systems (WCCS), Marrakech, 2015, pp. 1-7, doi: 10.1109/ICoCS.2015.7483283.
- [8] R. Das and T. H. Morris, "Machine Learning and Cyber Security," 2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, 2017, pp. 1-7, doi: 10.1109/ICCECE.2017.8526232.
- [9] I. Duic, V. Cvrtila and T. Ivanjko, "International cyber security challenges," 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2017, pp. 1309-1313, doi: 10.23919/MIPRO.2017.7973625.
- [10] D. Ratasac, F. Khalid, F. Geissler, R. Grosu, M. Shafique and E. Bartocci, "A Roadmap Toward the Resilient Internet of Things for Cyber-Physical Systems," in *IEEE Access*, vol. 7, pp. 13260-13283, 2019, doi: 10.1109/ACCESS.2019.2891969.
- [11] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K. -K. R. Choo and R. M. Parizi, "An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic," in *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8852-8859, Sept. 2020, doi: 10.1109/JIOT.2020.2996425.
- [12] A. Sivanathan, H. H. Gharakheili and V. Sivaraman, "Detecting Behavioral Change of IoT Devices Using Clustering-Based Network Traffic Modeling," in *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7295-7309, Aug. 2020, doi: 10.1109/JIOT.2020.2984030.
- [13] Na Liu, Alexandros Nikitas, Simon Parkinson, Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach, *Transportation Research Part F: Traffic Psychology and Behaviour*, Volume 75, 2020, Pages 66-86, ISSN 1369-8478, <https://doi.org/10.1016/j.trf.2020.09.019>.
- [14] Isabel Arend, Asaf Shabtai, Tali Idan, Ruty Keinan, Yoella Bereby-Meyer, Passive- and not active-risk tendencies predict cyber security behavior, *Computers & Security*, Volume 97, 2020, 101964, ISSN 0167-4048.
- [15] Wang, W., Harrou, F., Bouyeddou, B. et al. A stacked deep learning approach to cyber-attacks detection in industrial systems: application to power system and gas pipeline systems. *Cluster Comput* 25, 561–578 (2022). <https://doi.org/10.1007/s10586-021-03426-w>.
- [16] Alkahtani, H. and Aldhyani, T., 2021. Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications. *Security and Communication Networks*, 2021, pp. 1-23.
- [17] F. Hossain, M. Akter and M. N. Uddin, "Cyber Attack Detection Model (CADM) Based on Machine Learning Approach," 2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), 2021, pp. 567-572, doi: 10.1109/ICREST51555.2021.9331094.
- [18] K. R. Choo, M. Conti and A. Dehghantanha, "Special Issue on Big Data Applications in Cyber Security and Threat Intelligence – Part 1," in *IEEE Transactions on Big Data*, vol. 5, no. 3, pp. 279-281, 1 Sept. 2019, doi: 10.1109/TBDATA.2019.2933039.
- [19] S. Merat and W. Almuhtadi, "Artificial intelligence application for improving cyber-security acquirement," 2015 IEEE 28th Canadian Conference on Electrical and Computer Engineering (CCECE), Halifax, NS, 2015, pp. 1445-1450, doi: 10.1109/CCECE.2015.7129493.