Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Research Trends In Deep Learning and Machine Learning for Cloud Computing Security

Shoaib[1]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
shoaib03969@gmail.com

Mohsin Ali[2]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
mohsinali46776@gmail.com

Junaid Baber[3]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
junaidbabar121@gmail.com

Zain ul Abidien[4]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
Malikzain1122awan@gmail.com

Muavia Hasan[5]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
Muaviahassan67@gmail.com

Abstract

Meanwhile, security concerns of cloud computing services have grown more diverse and pressurizing with evolution of existing cloud services known to overtake traditional security solutions. Consequently, this paper aims at identifying the contribution of the two most crucial advanced technologies known as machine learning and deep learning in strengthening cloud security. These are techniques that use Artificial Intelligence to detect threats and respond to, or prevent them, automating the identification of abnormalities in cloud traffic. This study focuses on discussing how ML and DL work and their uses, such as fraud detection, real-time authentication in the Zero Trust models, and building security into an application at the software development stage. In addition, it covers important aspects that were previously omitted in other surveys of DL, including privacy, and describes important methods for DL privacy, including federated learning and homomorphic encryption. The paper also explores the issue of model interpretability before highlighting the need for explainable AI frameworks in order to confidence the security administrators. Besides, it explores the threat of adversarial attacks against ML models and also presents a guide to improving model resilience. In conclusion, it is recommended that continuous research should be conducted, and cooperation between researches, practitioners, and policy makers establish to come up with effective and dynamic secure cloud solutions.

Keywords: Machine Learning, Deep Learning, Cloud Computing, Software Development, AI framework, Cloud traffic, Cloud security,

Introduction

The security risks with cloud solutions are ever on the rise as the adoption of cloud solutions across different fields continues to grow. Current security processes and measures are rendered ineffective by advancements in cloud technologies which are advancing at an alarming pace, increasing vulnerability of an organization's information infrastructure to high level threats. This growing concern means that cloud security must be improved by embracing the best technologies available, with the machine learning (ML) / deep learning (DL) being central to cloud security [1, 5].

AI and specifically machine learning and deep learning propose fresh ways of approaching threat detection, response, as well as prevention in the cloud. Due to massive data, these technologies can analyze cloud traffic, determine deviations, and initiate actions on threats. For example, using the ML algorithms, one can always monitor user behavior patterns that may involve fraudulent activities concurrently through the analysis of the ML algorithms result list, the DL models can also improve a list of intrusion detection system accuracy by recognizing other patterns indicative of the security breach. Theirs's research article seeks to analyse the current trends in ML and DL in CCSS in terms of application of the technology, advantages observed and limitations encountered [6, 10].

More specifically, it will focus on more sensitive subjects like the reacting on threats in real time, the practicing of fraud detection, monitoring of the data protection of its users. The paper will also highlight features that previous studies have left out; the interpretability of the model and need for the security administrators to have a measure of trust in the AI frameworks used [11].

Furthermore, this paper will explore what privacy concerns exist while using deep learning in cloud security, including positive approaches such as federated learning and homomorphic encryption that can preserve the privacy of consumer information in case of reselling but also enhance cloud security measures. Moreover, the article will touch upon the topic of adversarial attacks on ML models and will describe ways to increase models' resistance to such threats [12].

In order to respond to these issues, predictive network maintenance using Artificial Intelligence (AI) and Machine Learning (ML) has thus developed into a potential solution. By analyzing vast amounts of both historical data and real-time network data, improve AI/ML algorithms can help to identify patterns, prevent potential failures and provide valuable recommendations before the problems worsen. This proactive approach proactively helps to prevent highly undesired events, allocate network resources more effectively, cut maintenance expenses, and improve the whole stability of network services. Time series forecasting methods including LSTM deep learning models can be helpful in modeling future network behaviors while autonomous classification methods, including Random Forest or SVM can recognize anomalous signs that might be indicative of impending failures [13].

Literature Review

There are numerous prior works and literatures that have examined distinct perspectives of AI/ML in co network management addressing aspects like traffic forecasting, anomalous phenomena identification, and self-configuration of network settings. Yet, there exist a research gap in the area of predictive maintenance specifically to quantify the performance of various AI/ML methods. For instance, Deep Learning models such as LSTM network have been used in time series forecasting, Random forest and SVM for classification and anomaly detection. However, a systematic comparison of these algorithms for predictive maintenance in networks is still limited [14].

Over the last few years, many researchers have focused on investigating the relevance and use of Artificial Intelligence (AI) and Machine Learning (ML) data networks in particular, in areas like traffic prediction, anomaly detection as well as automatic network configuration. Even though these improvements have highly changed the efficiency and the security in networks, there is a clear lack of research in the field of predictive maintenance, especially, concerning the comparison of the basic AI/ML methods for its solution [15, 20].

The key role of managing the network is to predict the possible problem and solve them before they become critical hence reducing time wastage and improving the general performance of the network. However, to the best of the author's knowledge, there is a lack of literature concerning performance comparison of different AI/ML algorithms for PM in the networking context. This becomes apparent when one has to subdivide existing studies based on the fact that while they cover applications such as traffic optimization as well as real-time anomaly detection, they lack a thorough analysis of and its applicability to different types of predictive maintenance techniques [21, 22].

Furthermore, network automation platforms, Cisco DNAC enter by Cisco and Mist AI by Juniper also incorporate ML-based analytics for network insights even though the ML is hosted for monitoring rather than for predictive maintenance. This research seeks to fill this gap by presenting a comprehensive analysis of several AI/ML strategies particularly for predictive network maintenance [23].

In the time series forecasting, the succeeding Deep Learning model of Long Short-Term Memory (LSTM) network has promising results to offer. These models are especially good in computing long-term dependencies that makes it proper for predicting future problems in a network. However, others are Random forest, and Support Vector Machine (SVM), which are famous for their performance in classification and anomaly detection. Random Forest, using an ensemble of learning format, will take high dimensionality data, whereas SVM excels in the complex separation of datasets. With these capabilities, there se merges the search that comprehensively compares how these models efficiently conducts predictive maintenance on networks [24, 28].

To fill this gap, the current research seeks to offer a comprehensive assessment of different AI/ML methods especially for predictive network maintenance. By using the above aspects of performance appraisal, we make a comparison of the performance [29, 30].

Other models like, LSTM, Random forest, SVM, the effectiveness of these models in predicting the fails of the network and also reducing the maintenance of the network will be tested and compared in this study. To achieve this aim, the best AI/ML approaches for proactive network reliability analysis for predictive maintenance will be identified with the view of improving on building of self-healing intelligent network systems. This will provide the study's utility in helping network administrators in the implementation of predictive maintenance solutions within their network infrastructure [30, 33]

The current research shall employ a qualitative approach and shall therefore rely on semi-structured interviews and case studies which will be responded to by the network engineers, IT managers, and AI/ML specialists. This design is selected so as to obtain detailed descriptions of the practical application of AI/ML strategies for PM, and their contexts [34, 37].

Problem Definition

Identify the specific task in computer networking where ML/DL can provide a solution:

Examples: Traffic categorization, anomaly identification, intrusion detection systems, traffic characterization for optimization, prognostic and health management.

Data Collection and Preprocessing

Data Sources: Packet captures, flow data, interface statistics, system counters and audit logs, Web site traffic, and user activity patterns [38, 40].

Data Cleaning: Cleaning the data involves; deleting noise, dealing with the missing values and data balancing [41].

Feature Engineering: Of course, there they extract primary characteristics like packet, size, latency, protocols and topology of the network connection.

Normalization: Normalization to make an input to ML/DL models more standard and to expand its range of values [42].

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Model Selection

Supervised Learning: Applied when you have labeled data which is seldom the case in natural language processing (such as classifying traffic type).

Algorithms: Decision Trees, Support Vector Machines (SVM), Random Forest, k-Nearest Neighbors (KNN) [43].

Unsupervised Learning: Responsible for clustering and the identification of anomalies when there are no labels.

Algorithms: k-Means: DBSCAN; Auto encoders.

Reinforcement Learning (RL): Engaged within the network and mainly used in the role of dynamic routing [44].

Deep Learning Models: Used in treatment of large problems and large problem solving [45].

Models: Convolutional Neural Networks, CNNS for images, Recurrent Neural Networks and Long Short Term Memory, LSTM for flow data such as traffic data, Graph Neural Networks, GNNs for analyzing network topology [46, 49].

Model Training

Training Data: Divide data into train and cross-validation set and test set. **Optimization:** There are quite a number of optimization that you could use such as gradient descent and others like Adam, RMSprop.

Model Evaluation and Validation

Metrics: Use of performance measures such as accuracy, precision, recall, F1 score, and ROC-AUC for classification problems; mean squared error for regression.

Cross-Validation: In order to prevent overfitting, use k-fold cross-validation.

Deployment and Integration

Integration: Integrate models in the existing systems within the network so that integration is harmonious.

Monitoring: Always check on the performance and the Models can be trained on new data the same way.

Use Cases in Computer Networks

Traffic Classification: Explain discovery of applications and services using traffic analysis.

Anomaly Detection: Experience highly unsupervised signals, which could reveal other security threats.

Intrusion Detection Systems (IDS): Preventing and tracking single and combined type malicious activities.

QoS Optimization: Allocate resources entity and bandwidth more efficiently.

Predictive Maintenance: Preventive maintenance of Network Equipment's and Scheduling.

Challenges and Recommendations

Applications of AI/ML for predictive network maintenances; come with some disadvantages including privacy issues, skills required and costs of implementation as some of areas of concern. The challenges that will be spelt out by this research and strategies of addressing them will include; training investment, cloud solution to support growth, and data management governance.

Conclusion and Future Directions

It may be critically imperative to use big data and machine learning to increase cloud security through the effective deployment of models to detect threats in large scale cloud environments in real time. Approaches common as model pruning, quantization, transfer learning, edge computing integration and model compression greatly enhance scalability, efficiency, and speed in the application of driven ML. Nevertheless, some issues are still open, and they are connected mainly with the increased mobility and flexibility of cloud environments. Further studies should address issues of designing more flexible models that suit different configurations of clouds and self-tuning models to optimize scaling procedures with less impact on the overall performance. The deep learning helps to improve the threat detection and response capabilities of cloud security. Still, privacy concerns play a role as the data used is sensitive and prone to leakage. Privacy-preserving methods including federated learning, differential privacy, homomorphic encryption and secure multi-party computation are mature techniques capable of addressing these data-to-privacy risk issues. Cloud De-Identification Defend against Model Inversion Attacks: Cloud systems can accommodate user data efficiently and protect system privacy by embedding these strategies in deep learning model design. However, it is important to adopt these technical privacy-preserving methods which are key for making sure that deep learning models of cloud security can be effectively trained as well while being respectful of data privacy concerns.

The use of deep learning (DL) and machine learning (ML) in the cloud computing security region is getting popular with development potential and risks. Thus, security effectively remains a critical factor since as cloud usage rises, more improved threats emerge. ML and DL improve threat identification and response, and data privacy through 'model pruning' and 'transferring' techniques ensuring high throughputs in operational large scales. However, privacy issue is a drawback from the use of DL models since it violate the privacy of the users hence, the privacy preserving methods such as the federated learning and homomorphic encryption come in handy to avoid leakage of data and model inversion attacks. Furthermore, the obscurity of many of the ML algorithms present a distrust from security administrators that can be solved through the introduction of the explainable AI frameworks. The threats are also present in faking and adversarial attacks on the ML models where adversarial training and input preprocessing help to solve these problems. Nonetheless, it is clear that both ML and DL hold great promise for the future of cloud security, but pointed attention must be paid to the development of these technologies, as well as to improving their algorithms, methodologies, and usability in large scale applications, methods for preserving the privacy of their algorithms, and novel strategies for addressing adversarial threats. It is therefore crucial to involve researchers as well as practitioners and policymakers to enhance the process of translating knowledge into practice as well as integrating the same into the changing terrorisms' systems.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Khan, A. Yasmeen, S. Jan, U. Hashmi, "ENHANCED RESOURCE LEVELING INDYNAMIC POWER MANAGEMENT TECHNIQUEOF IMPROVEMENT IN PERFORMANCE FOR MULTI-CORE PROCESSORS" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

[2] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

[3] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[4] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

[5] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

[6] Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

[7] M. S. Abdul Razak, S. P. A. Gothandapani, N. Kamal, and K. Chellappan, "Presenting the Secure Collapsible Makerspace with Biometric Authentication", Eng. Technol. Appl. Sci. Res., vol. 14, no. 1, pp. 12880–12886, Feb. 2024.

[8] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

[9] Amangele, P., Reed, M. J., Al-Naday, M., Thomos, N., & Nowak, M. (2019). Hierarchical Machine Learning for IoT Anomaly Detection in SDN. In2019 International Conference on Information Technologies (InfoTech). 1-4. IEEE.

[10] Anderson, J. P. (1980). Computer security threat monitoring and surveillance.Technical Report, Fort Washington, PA, James P. Anderson Co.

[11] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

[12] Aburomman, A. A., &Reaz, M. B. I. (2017). A survey of intrusion detection systems based on ensemble and hybrid classifiers.Computers & Security,65, 135-152.

[13] Agrawal, S., & Agrawal, J. (2015). Survey on anomaly detection using data mining techniques.Procedia Computer Science,60, 708-713.

[14] Ahmad, S., Lavin, A., Purdy, S., & Agha, Z. (2017). Unsupervised real-time anomaly detection for streaming data.Neurocomputing,262, 134-147.

[15] Akhi, A. B., Kanon, E. J., Kabir, A., &Banu, A. (2019).Network Intrusion Classification Employing Machine Learning: A Survey. (Doctoral dissertation)Department of Computer Science and Engineering, United International University, Bangladesh.

[16] Alizadeh, H., Khoshrou, A., &Zuquete, A. (2015). Traffic classification and verification using unsupervised learning of Gaussian Mixture Models. In2015 IEEE international workshop on measurements & networking (M&N). 1-6. IEEE. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

[17] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[18] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

[19] Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

[20] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[21] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power

plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[22] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

[23] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

[24] Aung, Y. Y., & Min, M. M (2018). An analysis of K-means algorithm based network intrusion detection system. Advances in Science, Technology and Engineering Systems Journal,3(1), 496-501. Bauer, F. C., Muir, D. R., &Indiveri, G (2019). Real-Time Ultra-Low Power ECG Anomaly Detection

[25] Bhati, B. S., Rai, C. S., Balamurugan, B., & Al-Turjman, F. (2020). An intrusion detection scheme based on the ensemble of discriminant classifiers.Computers & Electrical Engineering,86, 106742.

[26] Bhattacharyya, D. K., &Kalita, J. K. (2013).Network anomaly detection: A machine learning perspective. CRCPress.

[27] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[28] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[29] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[30] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[31] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

[32] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[33] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

[34] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[35] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

[36] Haripriya, L.A., Jabbar, M., &Seetharamulu, B. (2018). A Novel Intrusion Detection System Using Artificial Neural Networks and Feature Subset Selection. International Journal of Engineering and Technology, 7(4), 181. http://doi.org/10.14419/ijet.v7i4.6.20458

[37] Hoang, D. H., & Nguyen, H. D. (2018). A PCA-based method for IoT network traffic anomaly detection. In2018 20th International Conference on Advanced Communication Technology (ICACT), 381-386. IEEE.

[38] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson,

R. (2016). Threat analysis of IoT networks using artificial neural network intrusiondetection system. In2016 International Symposium on Networks, Computers and Communications (ISNCC), 1-6. IEEE.

[39] Blanco, R., Malagón, P., Briongos, S., & Moya, J. M. (2019). Anomaly Detection Using Gaussian Mixture Probability Model to Implement Intrusion Detection System. InInternational Conference on Hybrid Artificial Intelligence Systems, 648-659. Springer, Cham.

[40] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey.ACM Computing Surveys (CSUR),41(3), 1-58.

[41] Chauhan, P., & Shukla, M. (2015). A review on outlier detection techniques on data stream by using different approaches of K-Means algorithm. In2015 International Conference on Advances in Computer Engineering and Applications. 580-585. IEEE.

[42] Chen, C. M., Guan, D. J., Huang, Y. Z., &Ou, Y. H. (2016). Anomaly network intrusion detection using hidden Markov model.International Journal of Innovative Computing, Information and Control,12, 569-580.

[43] Chew, Y. J., Ooi, S. Y., Wong, K. S., & Pang, Y. H. (2020). Decision Tree with Sensitive Pruning in Network-based Intrusion Detection System. InComputational Science and Technology, 1-10. Springer, Singapore.

[44] Ding, M., & Tian, H. (2016). PCA-based network traffic anomaly detection.Tsinghua Science and Technology,21(5), 500-509.

[45] Dua, S., & Du, X. (2016).Data mining and machine learning in cybersecurity. CRC press.ernandes G., Rodrigues, J. J., Carvalho, L. F., Al-Muhtadi, J. F., &Proença, M. L. (2019). A comprehensive survey on network anomaly detection.Telecommunication Systems,70(3), 447-489.

[46] Gu, J., Wang, L., Wang, H., & Wang, S. (2019). A novel approach to intrusion detection using SVM ensemble with feature augmentation.Computers & Security,86, 53-62.

[47] Han, X., Xu, L., Ren, M., &Gu, W. (2015). A Naive Bayesian network intrusion detection algorithm based on Principal Component Analysis. In2015 7th International Conference on Information Technology in Medicine and Education (ITME), 325-328. IEEE.

[48] Hu, J., Ma, D., Liu, C., Shi, Z., Yan, H., & Hu, C. (2019). Network Security Situation Prediction Based on MR-SVM.IEEE Access,7, 130937-130945.

[49] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019