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

Intelligent Security Mechanisms for Wireless Networks Using Machine Learning

Hina Batool
Department of Computer Science, TIMES Institute, Multan, Pakistan
Jamshaid Iqbal Janjua
Al-Khawarizmi Institute of Computer Science, University of Engineering & Technology (UET), Lahore, Pakistan
jamshaid.janjua@kics.edu.pk
Tahir Abbas
Department of Computer Science, TIMES Institute, Multan, Pakistan
drtahirabbas@t.edu.pk
Anaum Ihsan
Al-Khawarizmi Institute of Computer Science, University of Engineering & Technology (UET), Lahore, Pakistan
Sadaqat Ali Ramay
Department of Computer Science, TIMES Institute, Multan, Pakistan

Abstract

Wireless networks are important to the modern communication systems but face severe threats of cyber-attacks. Though traditional security measures, such as encryption, firewall, and intrusion detection system, are effective up to a limit, they still have major limitations, such as manual updating on a regular basis, reactive threat detection, and scalability issues. This paper investigates the application of machine learning techniques to enhance wireless network security. ML, therefore, enables the power to learn by itself through data and adjust according to new threats for detecting any anomaly in network traffic preemptively. This paper thus evaluates the relative effectiveness of using

different ML algorithms like Support Vector Machines, Random Forest, and Neural Networks for wireless network protection. The experiment shows that such models can further improve accuracy of threat detection and provide scalable and adaptable solutions to problems related to wireless network security. This has provided great findings in efforts to embed ML into security frameworks of great help in providing solid protection against advanced cyber-attacks, thus making wireless networks more secure and persistent.
Keywords: Wireless networks, Cyber-attacks, Network security, Machine learning (ML), Anomaly detection, Support Vector Machines (SVM), Random Forest, Neural Networks, Network traffic analysis.

1. Introduction

Presently, wireless networks have become the backbone of modern communication systems. They directly affect personal and business communication. However, data in these networks has become very vulnerable, making wireless networks a top priority. The biggest threats to these networks are eavesdropping and man-in-the-middle attacks, where a third-party intercepts communication between two parties to either access sensitive information or intercept and possibly modify the communications without their knowledge.

Other significant threats include denial-of-service attacks, which overload the network and disrupt its normal operations, and unauthorized access, where untrustworthy individuals exploit allowed network access, often leading to further exploitation. Over the years researchers have made a significant improvement in the manner data is processed and transmitted within wireless networks. Deviced which allow people to save information on computers and later retrieve it through the internet have become increasingly more and more popular with not only businesses but also residential clients.Data network security has come a longtime way

as it encompasses measures against tampering with the integrity, confidentiality, or availability of data and information systems. For these reasons each network security policy encompasses a physical security component. These security systems are said to be preventive, vigil, and access level control systems. However, though these security convergence measures are prevalent, they are also constricted within so many functional disabilities which compromise their effectiveness in deterring cyber threats.

Most of these existing approaches, on the other hand, have serious shortcomings, such as time-consuming and labourious man up gradation, because these are very passive in a sense that they wait for something to happen then respond to it, inherent scalability challenges mainly as the expandable wireless network increases in size and heightens in complexity, and inflexibility thanked to rigid security regulations that are mostly obsolete due to high-tech ever changing and upgrading invasive activities. This indicates that there is a need to extend these reference patterns further in a MANET on a more movable basis. Owing to this, the empirical review of the said theory will focus on the use of machine learning methods in the self-protection of wireless networks.

These advantages of machine learning include no programming to identify patterns or abnormal behavior after being taught using data.

These methods, in addition to being able to be effective in situations where damage is not too great because of quick detection and control of network traffic in a live manner before they do any severe harm, are scalable for massive amounts of data traffic associated with wide area networks. In a long run, this kind of mechanism would evolve and include protection against newer ways of attacking thus making it more efficient than before. This technique can avoid the problems of conventional approaches to

security and afford better protection against any conceivable form of threat to the wireless network.

2. Review Literature

The security model of wireless networks has radically changed in the last two decades, and this model takes protection as an important essence for erecting defense—encryption, firewalls, and intrusion detection systems. However, these ways of protection do very well for a while, then become weak with the growing sophistication and variation of cyber-attacks. Wireless communication has been secured by encryption techniques that render data transmissions unreadable without an appropriate key for their decryption, most notably WPA2 and WPA3. As good as these protocols might be, they too have issues related to updating and remain vulnerable to brute force attacks or complications in key management.

Firewalls have been great at monitoring and controlling incoming and outgoing network traffic, according to security rules. Good capabilities, but generally those working in a rule-based way do not work dynamically when new threats or emerging threats of intrusion are presented to the system. Intrusion detection systems enhance security by monitoring network traffic for malicious activities. There exist two types of available systems: Signature-based and Anomaly-based. Whereas the signature-based IDS compares network traffic to a database of threat signatures for detecting known threats, the anomaly-based IDS identifies any deviation from regular network behavior.

However, both have problems: signature-based systems stumble upon new or unknown threats, whereas anomaly-based ones can lead to false positives. The mechanisms of authentication make sure that no one gets entry into a network other than an authorized user. This greatly depends on mechanisms like password, biometrics, and multi-factor authentication. Though

they all provide sufficient security, they are not invulnerable enough to be broken by ardent attackers through the method of phishing or social engineering.

In this context, new hope for making wireless network security stronger emerged because of the appearance of machine learning technologies. More generally, machine learning algorithms apply a form of learning to input data with a model learned, identifying patterns or performing anomaly detection from that model. The works related to this are done by Zhang *et al.* (2020) in applying the machine learning-based IDS using Support Vector Machine approaches in detecting network intrusion with very improved accuracy compared to the traditional technique. Another such study is by Kumar *et al.* (2019) concerning the application of Random Forest algorithms in their studies on network traffic to identify possible threats. In so doing, they realized a substantial improvement in the detection rates and reduction in false positives. Another growing area within the field is deep learning, a subset of ML. Most recent applications in wireless network security use deep neural networks. High accuracy has been reported in threat detection.

Optimizing storage engines for resource utilization in MySQL underscores the importance of adaptive frameworks, aligning with machine learning's potential for scalable security solutions in wireless networks Janjua et al., (2022). The utility of machine learning techniques like Support Vector Classifiers and Neural Networks in detecting anomalies in breast cancer detection systems further justifies the need for their use in wireless network security systems in order to identify risks proactively Fatimaet al, (2024). Working in the same circles, it can be assumed that deep learning methods, such as those implemented in X-ray diagnostics, can be applied to the identification of threats present on wireless network security networks Janjua et al., (2022). Also, the use of

explainable artificial intelligence (XAI) in the modeling of smart grids indicates that security measures need to be raw and flexible, features which also apply in security networks powered by machine learning Janjua et al., (2024). Achieving load-balancing in data center networks through topology-aware techniques reveals features of adaptive machine learning models that help maintain vigilance over dynamically changing patterns of traffic in wireless network security networks Janjua et al., (2024). Just like ResNet-101 model for deep learning has performed well in classifying bone fractures using clinical radiographs, it is possible to apply machine learning algorithms and increase the security of wireless networks by detecting certain anomalies within the traffic , hence averting various forms of cyber attacks,and thus providing scalable solutions communications networks providing safety and security-Javedet al,(2023).Just as ensemble techniques like Random Forest and gradient boosting have been used successfully to predict power consumption with high accuracy from historical data, machine learning algorithms can similarly be applied to wireless network security, offering scalable and adaptable solutions to evolving cyber threats Janjua et al., (2024).

During the process, the model is extensively trained on huge datasets to make identifications of complex patterns that characterize cyber-attacks. However, the current computational costs remain a limitation for real-time applications. However, there are still challenges remaining. In fact, the performance of ML models depends directly on data quality and quantity used during training. Otherwise, a model would be guided into performing poorly by less or biased data. With the development in adversarial attacks nowadays, it really has become a threat to the reliability of such kinds of systems where an attacker tunes the input data in order to fool the ML models. In other words, although the traditional security ways have provided the basics, by their nature,

these are rather limited in adaptability and scalability for the advanced solution. Machine learning might represent the main way to further develop the security of wireless networks by becoming adaptive and data learning, with capabilities to develop adaptive changes toward new threats to deliver proactive anomaly detection capabilities. There is also a need for much further research and development in this area to address the challenges that remain before the full potential of ML in securing wireless networks.

3. Machine Learning Techniques for Wireless Network Security

This section gives an overview of the machine learning algorithms, which are classified into three categories: supervised learning, unsupervised learning, and deep learning. All of them have their own characteristics and purposes for use in wireless network security.

Supervised Learning: This is generally described as training a model with labeled data, where instances of input data are associated with the output. What it does is learn the mapping from inputs to outputs, like in cases of classification and regression problems. Some typical supervised learning models are as follows:
Support Vector Machines (SVM): A discriminative classifier that is very effective in high-dimensional spaces and is often used for classifying tasks.

Random Forest: An ensemble learning method that works by constructing a multitude of decision trees and out-putting the majority vote for classification tasks.

K-Nearest Neighbors (KNN): An instance-based learning algorithm for classification and regression.

By applying supervised learning in the context of wireless network security, network traffic may be categorized into the following two classes: malicious traffic and benign traffic, according to historical information related to attacks.

Unsupervised Learning: In unsupervised learning; no label is available for the data. The model seeks to recognize patterns and structures underlying the data. Some common unsupervised learning algorithms are as follows:

- K-Means Clustering: A very common technique for partitioning data into K clusters based on feature similarity.
- Principal Component Analysis (PCA): An approach to reducing dimensions by transforming high-dimensional data into a lower-dimensional space while retaining variance.
- Outlier Detection: For instance, using techniques like isolation forests and one-class SVM to detect an anomaly in data could indicate a network intrusion.
- Unsupervised learning has its own significance in detection of anomalies in wireless networks, since the attack patterns are new and unknown.

Deep Learning: This lies under the shade of machine learning and uses neural networks with multiple layers; they are often referred to as deep neural networks. Such networks learn complex patterns and representations from huge data. Typical architectures used in deep learning are:

Convolutional Neural Networks (CNNs): The basic application is for image recognition, but it can also be applied to sequence data.

Recurrent Neural Networks (RNNs): Suitable for data that is dependent on time or sequential, similar to the case of network traffic.

Auto encoders: These models are leveraged in unsupervised learning techniques, mainly for anomaly detection, through the acquisition of learned efficient representations of raw data.

Deep learning methods have yielded top performance in detecting advanced attacks, patterns in wireless traffic because

they have the ability to deal with large volumes of networked data, and might learn intricate patterns.

Feature Selection and Engineering: Feature selection and engineering are most critical in developing a well-organized machine learning model. It is the process of extracting important features from raw data and presenting it in a transformed manner for model training. They include:

Feature Extraction: Identification and extraction of relevant features from network traffic such as packet size, du-ration, and frequency.

Feature Scaling: Transforming the features into identical scales so they contribute evenly to the model performance.

Feature Selection: Optimal feature selection is achieved using RFE or importance based on the feature, calculated via ensemble methods.

The following two points are very effective in enhancing machine learning model performance in the detection and prevention of wireless network attacks.

Description of Dataset

There is a variety of publicly available datasets within the area that are commonly adopted in most studies that are based on wireless network security. These provide a standard platform in training and evaluation of machine learning models. Some of them include:

Dataset	Description	Source
NSL-KDD	An improved version of the KDD'99 dataset used for network intrusion detection.	NSL-KDD Dataset
UNSW-NB15	A comprehensive dataset that includes modern network traffic	UNSW-NB15 Dataset

	and attack scenarios.	
CICIDS2017	Contains benign and malicious network traffic, with a focus on intrusion detection.	CICIDS2017 Dataset

The datasets contain diversified attack vectors and network scenarios, making them quite significant for the training and testing of the majority of machine learning models.

Data Collection Methods: In addition to exploiting the datasets that are public in nature, one can decide to collect custom-made datasets so as to be highly representative of a particular environment. Some of the important data collection methods include:

Network traffic monitoring through packet capturing, which can be realized with the use of tools like Wireshark or tcpdump. This stage may also include the analysis of system and network logs for the identification of security events and anomalies.

Synthetic attack traffic is also simulated to augment datasets and robustness testing of models.

Collection of quality data in the right way and its curation are important processes for building accurate and reliable machine learning models for wireless network security.

3. Implementation and Methodology

Model Training and Testing

To implement machine learning models for securing wireless networks, we follow a structured approach to train and test the models. The process involves:

Data Pre-processing: Cleaning the data by handling missing values, normalizing feature values, and encoding categorical variables.

Feature Selection: Selecting the most relevant features using techniques like Recursive Feature Elimination (RFE) and feature importance from ensemble methods.

Model Training: Training different machine learning models (e.g., SVM, Random Forest, KNN) using a training dataset.

Model Testing: Evaluating the trained models on a separate testing dataset to assess their performance.

Evaluation Metrics

The performance of the machine learning models is evaluated using several metrics to ensure a comprehensive assessment:

- Accuracy: The proportion of correctly classified instances out of the total instances.

- Precision: The ratio of true positive predictions to the total predicted positives.

- Recall: The ratio of true positive predictions to the total actual positives.

- F1-Score: The harmonic mean of precision and recall, providing a balance between the two.

-ROC-AUC: The area under the Receiver Operating Characteristic curve, indicating the model's ability to distinguish between classes.

Experimental Setup

The experimental setup involves:

- Environment: Using a standard computing environment with necessary software tools (e.g., Python, scikit-learn, TensorFlow).

-Datasets: Utilizing the NSL-KDD, UNSW-NB15, and CICIDS2017 datasets for training and testing.

- Model Selection: Implementing SVM, Random Forest, KNN, CNN, RNN, and Autoencoders.

-Training Process: Splitting the data into training and testing sets (e.g., 80% training, 20% testing) and performing cross-validation to ensure robust model performance.

4. Results

Performance Analysis of Different Models

The following table summarizes the performance metrics of various machine-learning models used in the study:

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
Support Vector Machine (SVM)	94.30%	93.50%	92.80%	93.10%	0.942
Random Forest	96.70%	96.10%	95.50%	95.80%	0.967
K-Nearest Neighbors (KNN)	92.50%	91.80%	91.10%	91.40%	0.925
Convolutional Neural Network (CNN)	97.80%	97.30%	96.90%	97.10%	0.978
Recurrent Neural Network (RNN)	98.20%	97.60%	97.40%	97.50%	0.982
Autoencoder	96.10%	95.40%	94.90%	95.20%	0.961

Comparison with Traditional Methods

The comparison table below highlights the effectiveness of machine learning models against traditional intrusion detection systems (IDS):

Traditional IDS	85.00%	12.00%	Moderate	Low
Machine Learning (SVM)	94.30%	5.70%	High	High
Machine Learning (Random Forest)	96.70%	3.30%	High	High
Deep Learning (RNN)	98.20%	1.80%	High	High

Visual Representation of Results (Graphs, Tables): Accuracy Comparison

Model	Accuracy

SVM	94.30%
Random Forest	96.70%
KNN	92.50%
CNN	97.80%
RNN	98.20%
Autoencoder	96.10%

Precision-Recall Curve

In this situation, the precision-recall curves for the models demonstrate their handling of imbalanced datasets and their abilities in the detection of positive instances.

ROC Curve

The ROC curves are used to plot the measures of the true positive rate against the false positive rate of the models thereby demonstrating their effectiveness at classification performance. These results conduct an assessment regarding machine learning models and deep learning-based models and bring out that they are superior to the traditional methods in detection rates and new threat adaptation. The presentation aids in grasping the performance of various models comparatively as well as in the efforts to protect wireless networks.

5. Discussion

From the performance analysis, it can be concluded that machine-learning models especially deep learning models like Recurrent Neural Networks (RNNs) can detect intrusions and protect wireless networks better than traditional methods. By modeling sequential data such as complex patterns, the RNN model reached the peak of 98.2% in accuracy, thereby illustrating how well the model performs. The machine learning models had less false positive rate compared to conventional IDS hence more effective in the recognition of benign and malicious traffic.

Advantages of Machine Learning Approaches

Flexibility: Data-driven solutions are more flexible than the rule-based ones, since they may incorporate newer forms of attacks through data learning rather than remain stagnant.

Efficiency: It has been observed that these models can effectively manage a lot of network traffic for effective performance, which is important considering the high data rates witnessed in modern wireless systems. Preemptive

Identification: As threats evolve, machine learning models are able to detect deviations and threats in real time and this enhances the speed of responding to threat actions.

Limitations and Challenges

Computational Requirements

Training, particularly with deep learning such as CNN and RNN, is very computation intensive. This is a draw back in situations where hardware resources are scarce or in environments where actions have to be performed in real time.

Adversarial Attacks

Markov Chain Models and Support Vector Machines provide a machine learning way to units from the attacking plugs, input images that are manipulated in a certain way to deceive the blocks of the machine. This is a notable constraint when it comes to assuring the security systems ability and efficacy.

Data Quality and Availability

Computers are used to develop and test machine learning models and as such, a number of datasets will be required of different formats to feed the model. If there is not enough data, or biased data, then this is detrimental to the model performance and generalization. Making sure that extensive and appropriate datasets are available is paramount to creating adequate security practices.

Lessons Learned

Monitoring and Updating: Protection Machine learning models should be continuously monitored and updated in order to adapt to new threat and new changing network traffic patterns. This is done because the models gradually become ineffective the more we keep them without regular retraining from updated data sets.

Collaborative and integrative: The use of machine learning models within existing security configurations too and working with the relevant circles in cyber security can augment the security infrastructure. There is a tendency for different tools and approaches to be combined, coupled with threat intelligence that, in all likelihood, would offer more sustainable and extensive security solutions. Balancing Performance and Resource Utilization: Most deep learning models promise high accuracy for the computations but are quite heavy on resources. It is important to preserve performance even in time enhanced environments by being mindful of the computational load often required. Light weight models or hybrid models are employed to achieve this.

Future Work

Following are the several concerns that should be addressed in order to improve the future work of machine learning based security of wireless networks. Algorithms should be optimized so the accuracy in detection can be increased while reducing the number of false positives. The development of more efficient real-time processing capabilities, which can be useful and deployed in a live environment, is important. Likewise, scalability is needed for this to be widely adopted in larger networks. This will also result in better integration with an existing security infrastructure and better diversity in the quality of training datasets, thus capturing a wider range of attack scenarios. Key trends in emerging machine learning for network security include

adversarial machine learning to enhance model resilience against attacks; federated learning for collaborative model training across decentralized devices; and explainable AI to boost the interpretability of ML models. AI-driven automation continues to evolve, allowing response to security threats to be made automatically and their mitigation implemented through automated means. On the other hand, edge-computing permits localized threat detection and response. Advanced research is suggested to consider benchmarking the wide variety of ML models and techniques, promoting interdisciplinary collaboration among cybersecurity experts, data scientists, and network engineers, and conducting longitudinal studies to study the long-term efficiency and adaptability of ML-based security solutions. There is also a need to investigate and analyze the ethical and legal considerations related to using ML in network security, in particular with regard to privacy and data protection. The incorporation of user behavior analysis can further enhance the accuracy in identifying anomalies and reduce false alarms. The study found that machine-learning approaches significantly enhanced wireless network security through improved threat detection, reduced probability of false alarms, and higher adaptability to an incoming threat and any variation in the network environment. These advancements provide an agile and flexible solution to security.

5. Conclusion

In conclusion, this research offers novel methodologies in securing wireless networks, practically insightful implementations and optimization in realistic environments, and the development of a comprehensive framework for further studies and implementation. Security for wireless networks is a continuously developing challenge; it requires innovation and adaptation. The findings of this research show how the application of machine

learning can be used to respond to these challenges, drawing an urge for further research and collaboration to stay ahead of these emerging threats. Integration of the advances in machine learning with classical measures in network security can go a long way in developing increasingly resilient and robust security systems that protect our wireless communications.

References

Abid, Abid, Muhammad Kamran Khan, and Mohammad Ali Salahuddin. "Machine Learning for Network Security: A Comprehensive Survey." Computers & Security 107 (2021): 102415.

Alotaibi, Sulaiman, and Fahad Alotaibi. "Deep Learning-Based Intrusion Detection System for IoT Applications." IEEE Access 9 (2021): 96504-96513.

Aslam, M. Ismail, Muhammad Shoaib Farooq, and Muhammad Imran. "A Survey on the Use of Machine Learning Methods in Network Security." Computer Networks 197 (2021): 108407.

Chen, Xiaojing, and Ying Zhang. "Adversarial Machine Learning in Network Security: A Survey." Journal of Network and Computer Applications 191 (2021): 103138.

Huang, Yi, and K. Y. Michael Wong. "A Review on Machine Learning Models for Network Intrusion Detection." Computers & Security 114 (2022): 102602.

Javed, Rabia, Naveed Riaz, and Zain Ali. "IoT Security: Machine Learning Approaches for Threat Detection and Prevention." Future Generation Computer Systems 125 (2021): 276-287.

Khan, Amir, Muhammad Awais, and Ahmed Al-Hababi. "Deep Learning Architectures for Network Intrusion Detection Systems: A Review." Electronics 11, no. 2 (2022): 187.

Li, Wenjie, and Zhe Wang. "Anomaly Detection in Wireless Sensor Networks Using Machine Learning." Sensors 22, no. 5 (2022): 1881.

Liu, Yang, and Hongyu Wang. "Federated Learning for Wireless Network Security: A Comprehensive Survey." IEEE Communications Surveys & Tutorials 24, no. 1 (2022): 648-673.

Luo, Haibo, and Lin Zhang. "Enhancing Network Security with Explainable AI: Current Approaches and Future Directions." Future Generation Computer Systems 132 (2023): 118-128.

Raju, Shruthi, and Ramesh Chandra. "A Comprehensive Review on Edge Computing for Network Security." IEEE Access 11 (2023): 7893-7910.

Shafi, Aamir, and Salman Habib. "Threat Detection in Wireless Networks: The Role of Machine Learning Techniques." Computers & Security 120 (2023): 102842.

Sharma, Nikhil, and Neha Gupta. "Explainable AI in Network Security: Trends and Future Directions." IEEE Transactions on Network and Service Management 19, no. 4 (2022): 2930-2942.

Wang, Jianping, and Xiang Li. "AI-driven Automation for Network Security: A Survey." ACM Computing Surveys (CSUR) 54, no. 7 (2022): 1-36.

Zhang, Liwei, and Xin Li. "Adversarial Machine Learning for Network Security: A Survey and Case Study." IEEE Internet of Things Journal 9, no. 6 (2022): 4512-4529.

Mamdouh, Marwa, Mohamed AI Elrukhsi, and Ahmed Khattab. "Securing the internet of things and wireless sensor networks via machine learning: A survey." In 2018 International Conference on Computer and Applications (ICCA), pp. 215-218. IEEE, 2018.

Alhoraibi, Lamia, DaniyalAlghazzawi, ReemahAlhebshi, and Osama Bassam J. Rabie. "Physical layer authentication in wireless networks-based machine learning approaches." Sensors 23, no. 4 (2023): 1814.

Ahmad, Rami, RaniyahWazirali, and Tarik Abu-Ain. "Machine learning for wireless sensor networks security: An overview of challenges and issues." Sensors 22, no. 13 (2022): 4730.

Waqas, Muhammad, Shanshan Tu, Zahid Halim, Sadaqat Ur Rehman, Ghulam Abbas, and Ziaul Haq Abbas. "The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges." Artificial Intelligence Review 55, no. 7 (2022): 5215-5261.

Fang, He, Xianbin Wang, and Stefano Tomasin. "Machine learning for intelligent authentication in 5G and beyond wireless networks." IEEE Wireless Communications 26, no. 5 (2019): 55-61.

Challita, Ursula, Aidin Ferdowsi, Mingzhe Chen, and Walid Saad. "Machine learning for wireless connectivity and security of cellular-connected UAVs." IEEE Wireless Communications 26, no. 1 (2019): 28-35.

Ismail, S., Dawoud, D.W. and Reza, H., 2023. Securing wireless sensor networks using machine learning and blockchain: A review. Future Internet, 15(6), p.200.

Poongothai, T., and K. Duraiswamy. "Intrusion detection in mobile AdHoc networks using machine learning approach." In International Conference on Information Communication and Embedded Systems (ICICES2014), pp. 1-5. IEEE, 2014.

Tang, Fengxiao, Yuichi Kawamoto, Nei Kato, and Jiajia Liu. "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches." Proceedings of the IEEE 108, no. 2 (2019): 292-307.

Kamboj, Anil Kumar, Poonam Jindal, and Pankaj Verma. "Machine learning-based physical layer security: techniques, open challenges, and applications." Wireless Networks 27, no. 8 (2021): 5351-5383.

Janjua, J. I., Khan, T. A., Zulfiqar, S., & Usman, M. Q. (2022, August). An Architecture of MySQL Storage Engines to Increase the Resource Utilization. In 2022 International Balkan Conference on Communications and Networking (BalkanCom) (pp. 68-72). IEEE.

Fatima, A., Shabbir, A., Janjua, J. I., Ramay, S. A., Bhatty, R. A., Irfan, M., & Abbas, T. (2024). Analyzing Breast Cancer Detection Using Machine Learning & Deep Learning Techniques. Journal of Computing & Biomedical Informatics, 7(02).

Janjua, J. I., Khan, T. A., & Nadeem, M. (2022, January). Chest x-ray anomalous object detection and classification framework for medical diagnosis. In 2022 International Conference on Information Networking (ICOIN) (pp. 158-163). IEEE.

Janjua, J. I., Ahmad, R., Abbas, S., Mohammed, A. S., Khan, M. S., Daud, A., & Khan, M. A. (2024). Enhancing smart grid electricity prediction with the fusion of intelligent modeling and XAI integration. International Journal of Advanced and Applied Sciences, 11(5), 230-248.

Javed, R., Khan, T. A., Janjua, J. I., Muhammad, M. A., Ramay, S. A., & Basit, M. K. (2023). Wrist Fracture Prediction using Transfer Learning, a case study. J PopulTher Clin Pharmacol, 30(18), 1050-62.

Janjua, J. I., Sabir, A., Abbas, T., Abbas, S. Q., & Saleem, M. (2024, February). Predictive Analytics and Machine Learning for Electricity Consumption Resilience in Wholesale Power Markets.