# AI Powered Post-Quantum Cryptography: Strengthening U.S. Cybersecurity with Quantum Computing

Mustakim Bin Aziz[1], Mani Prabha[2], Sweety Rani Dhar[2], Md Samiun[2], Rukshanda Rahman[1], SyedaFarjana Farabi[1], Ali Hassan[2], Syeda Kamari Noor[1]

Department of Business Administration, Westcliff University, San Francisco, CA 94104, USA[1]

Department of Business Administration, International American University, Los Angeles, CA 90010, USA[2]

Corresponding author: Mustakim Bin Aziz, Email: m.aziz.205@westcliff.edu

The rise of quantum computing threatens traditional cryptographic methods like RSA and ECC, which are vulnerable to quantum algorithms such as Shor's and Grover's. This study aims to assess cybersecurity vulnerabilities and enhance cyber threat detection using machine learning and deep learning techniques. The NSL-KDD dataset is employed for intrusion detection, utilizing feature selection methods like recursive feature elimination and mutual information analysis. This study proposed IntruDualNet which is Dual Output based deep learning model where it's predicted both binary and multiclass classification. Experimental results show high detection accuracy, with 99.70% for binary classification and 99.49% for multiclass classification, effectively identifying threats like DDoS, SQL injection, and XSS. The findings highlight the urgency of transitioning to post-quantum cryptographic standards and integrating AI-driven security solutions to mitigate emerging threats.

**Keywords:** IntruDualNet, Post-Quantum Cryptography, Cybersecurity, Quantum Computing, Intrusion Detection, Machine Learning.

2026. In Kusum Kumari Bharti & Noor Firdoos Jahan (eds.), *Next-Gen Data Analytics and Intelligent Automation*, 63–74. Computing & Intelligent Systems, SCRS, India. DOI: https://doi.org/10.56155/978-81-975670-6-3-6

# 1. Introduction

The digital world faces threat constantly in diverse situation. It is one of the most important concerns for individuals, business and governments alike. As cyber threats evolve and become more refined, ensuring the protection of sensitive data and communications is paramount. For many years, traditional cryptographic techniques such as RSA and Elliptic Curve Cryptography (ECC), have been backbone of secure digital communication. These techniques heavily depend on the mathematical complexity of specific issues like factoring large integers or resolving discrete logarithms, which is essential to tackle within a reasonable period using classical computers [1]. Quantum computing has exposed classical cryptography to substantial danger since its emergence. Quantum computers apply quantum mechanics to tackle problems through a mechanism that outpaces classical computers in terms of speed [2]. Shor's algorithm represents the biggest threat in quantum algorithms because it runs polynomial time factorizations of large numbers which completely exposed RSA and ECC to quantum assaults. Both Shor's algorithm and Grover's algorithm can connect via quantum speedup to attack symmetric-key cryptosystems through reduced effective key length effectiveness [3][4]. The threat to digital infrastructure security and global economic systems exists due to the direct impact of quantum computers. Research activities in Post-Quantum Cryptography (PQC) emerged because of rising quantum threats that motivated the development of quantum-resistant cryptographic methods. The goal of PQC involves creating cryptographic algorithms which defend against quantum computer operational strength. The algorithms function to protect data and communications from both classical and quantum attacks since they were built to resist quantum-powered threats. The process to shift from present classical cryptographic methods to quantum-resistant algorithms will need time to complete. The migration process requires a thorough assessment of current system vulnerabilities, as well as a discussion of how quantum computing poses risks to their weaknesses [5]. The necessity for this transition increases because classical cryptography remains the foundation which numerous worldwide organizations utilize to protect their sensitive data. Cryptographic systems function deeply within contemporary society because they protect financial information as well as health records and governmental communication networks. The threat from quantum computers to classical cryptography demands an immediate development of quantum-resistant cryptography standards that combine knowledge about encryption system risks and quantum computing capabilities [6]. A systematic examination of existing cybersecurity infrastructure weaknesses should be completed before moving forward with PQC solution deployment. Quantum computers produce more effective exploits against classical cryptographic systems whose weaknesses exist in current infrastructure. Quantum-powered cybersecurity will increase the danger level of established security threats like Distributed Denial of Service (DDoS), SQL injection and Cross-Site Scripting (XSS) attacks. Quantum computer advancement creates more effective attack opportunities against encryption schemes and security protocols, so it becomes crucial to evaluate system vulnerabilities to comprehend existing quantum security weaknesses [7][8]. Figure 1 visualizes Prioritizing Cybersecurity Threats and Vulnerabilities.

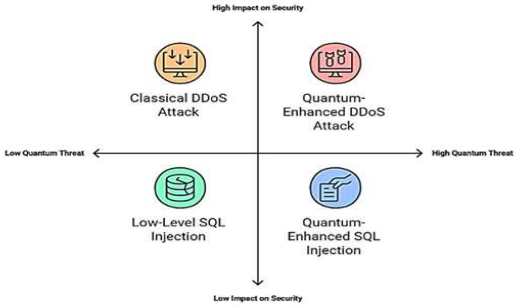


**Figure 1.** Prioritizing Cybersecurity Threats and Vulnerabilities.

On the other hand, machine learning models rely on large datasets to monitor security threats by identifying patterns and anomalies within database systems [9]. By training these models on network traffic data, analysts are able to detect a variety of attacks, including DDoS, SQL injection, and XSS—some of the most prevalent methods used by adversaries to breach systems [10]. Al Mazroa et al. [11] introduced an innovative method for automated cyberattack detection in a Cyber-Physical Systems (CPS) environment, known as Cyberattack Detection using Binary Metaheuristics with Deep Learning (ACAD-BMDL). This approach enhances CPS security through advanced cyberattack detection techniques. Similarly, Batchu et al. [12] proposed a novel deep learning framework for detecting DDoS attacks, which integrates phases of data pre-processing, balancing, and classification. This framework uses a stacked sparse denoising autoencoder in combination with a firefly-black widow hybrid optimization algorithm to significantly improve detection accuracy. In another study, Imran et al. [13] developed a hybrid model that merges Extreme Gradient Boosting (XGBoost) with convolutional neural networks (CNN) for feature extraction, followed by a combination with long short-term memory networks (LSTM) for classification. Kantharaju et al. [14] presented a machine learning-based intrusion detection framework that utilizes the Self-Attention Progressive Generative Adversarial Network (SAPGAN) for detecting security threats in IoT networks. This method achieves up to 27.55% higher accuracy and reduces computational time by 26.76%, outperforming traditional models by employing a modified War Strategy Optimization Algorithm and Local Least Squares for data preprocessing.

In light of these advancements, this research aims to address this critical gap by conducting a comprehensive vulnerability assessment of existing cybersecurity infrastructures through the application of machine and deep learning techniques. The study will perform both binary and multiclass classification for threat detection, providing insights into how current systems can be enhanced to effectively mitigate the risks posed by increasingly sophisticated adversarial methods.

## 1.1 Cyber Threats

The growth and development of digital infrastructure has triggered an equal development of assaults directed against it. Cyber threats advanced to target all network infrastructure components that include applications and data at an organization. Digital attacks create large-scale network outages as well as information theft which leads to long-lasting harm to reputation in addition to financial losses. The following section details prevalent dangerous cyber threats using three main examples: Distributed Denial of Service (DDoS), SQL Injection and Cross-Site Scripting (XSS) attacks.

### 1.1.1 Distributed Denial of Service (DDoS)

The Distributed Denial of Service (DDoS) attack stands as a destructive form of cyber threat against systems. Through this attack method hackers employ numerous contaminated systems which generate massive amounts of network traffic until the target system runs out of its resources and becomes inaccessible to normal users. Attackers execute this operation by taking control of botnets which represent a group of computer devices infected with malicious software. The targeted server receives overwhelming data packets from botnets which cause the server to degrade its performance until it stops functioning altogether. Through DDoS attacks systems which provide online services become paralyzed and business operations stop while major damage to organization reputation follows. The targeting capability of small businesses along with big organizations makes DDoS attacks a serious challenge for cybersecurity professionals. The rising complexity of these attacks requires more proactive defensive techniques which incorporate traffic observation alongside rate thresholds for control purposes [15].


**Figure 2.** DDoS Attack process

### 1.1.2 SQL Injection

SQL injection represents an effective time-tested attack which involves unwelcome SQL queries entered into text entry fields like search bars and login forms or URLs to disrupt a website's database systems.

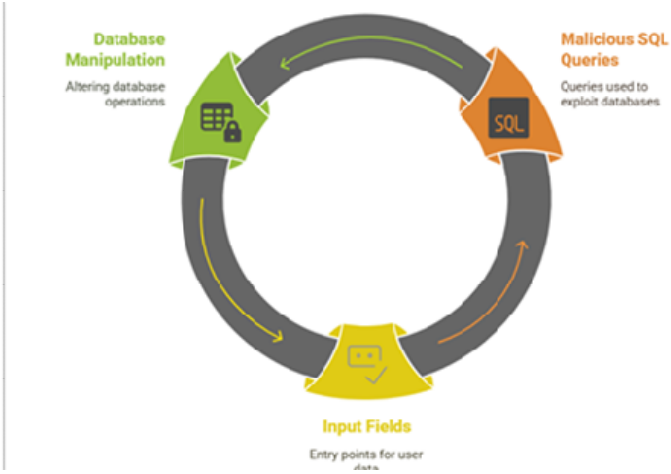


**Figure 3.** SQL Injection Threat Cycle

The presence of database query logic vulnerabilities gives attackers the opportunity to modify and access and delete sensitive website data. Through SQL injection attacks attackers gain access to steal multiple types of valuable information such as user login credentials together with credit card data and personal records. SQL injection has maintained its position as a serious threat to systems because businesses continue to fail at both validating user data properly and protecting their databases effectively. Illegal modification of database queries through unproperly sanitized user inputs allows attackers to obtain or change confidential stored information [16].

### 1.1.3 Cross-Site Scripting (XSS)

A Cross-Site Scripting (XSS) attack results when attackers embed malicious scripts especially JavaScript into web pages and applications. The executed scripts will run inside user browsers when they access the affected web page. Hackers exploit XSS attacks to secretly steal session cookies and login passwords and modify websites which results in website defacement and phishing users to fraudulent domains. The different forms of XSS attacks consist of Stored XSS, Reflected XSS and DOM-based XSS. The malicious script persists on the target server during Stored XSS attacks but Reflected XSS causes the script to reflect back from the web server before immediate execution. DOM-based XSS takes place when the vulnerable code exists in the client-side program instead of server-side resources. Malicious users exploit the trust users have in legitimate websites through the dangerous nature of XSS attacks [17].

## 2. Methodology

In this section, the methodology for this research is discussed, which follows a structured process that includes feature selection, model training, and evaluation. Figure 4 visualizes the proposed methodology.

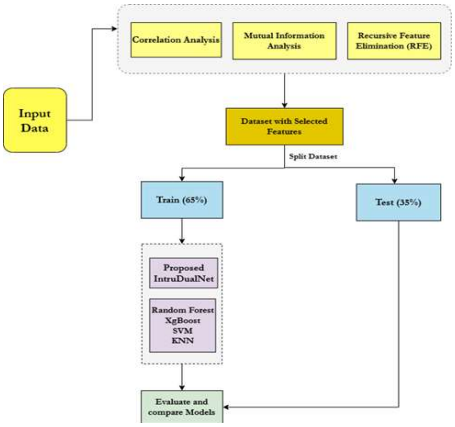


**Figure 4.** Proposed Methodology

### 2.1 Dataset

The NSL-KDD [17] dataset used in this study is an improved version of the original KDD'99 dataset, designed to address issues such as redundant records and class imbalances. The dataset contains 43 features (columns) and 125,972 instances (rows). The target column, representing the threat type, includes 22 attack categories and one normal class. For the purposes of this research, a threshold was set where any attack type occurring less than 200 times was classified under the "others" category. As a result, 11 distinct attack types, along with the normal class, were retained for multiclass classification. In the binary classification scenario, the "normal" class was distinguished from all other attack types, labeling everything else as "attacks."

### 2.2 Data Processing and Feature Selection

The data preprocessing process includes feature selection as its vital component because it helps improve model performance by discarding irrelevant or redundant features. The research implements

three vital feature selection methods which include Correlation Analysis and Mutual Information Analysis and Recursive Feature Elimination (RFE). The model benefits from these selection methods that pick vital features which lead to optimized prediction performance.

## 2.3 Correlation Analysis

A correlation analysis method helps identify features which demonstrate strong co-relationships that subsequently get removed from the dataset. The predictive model suffers downsides from multicollinearity when features exhibit strong interdependence. Research on variable associations requires the Pearson correlation coefficient to measure their statistical relationship [18]. Equation 1 shows the Pearson correlation co-efficient.

$$r = \frac{\Sigma(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\Sigma(X_i - \bar{X})^2 \Sigma(Y_i - \bar{Y})^2}} \quad (1)$$

## 2.4 Mutual Information Analysis

Mutual Information serves as a non-linear technique to evaluate variable dependencies through its measurement of shared information content. The information sharing between a feature and its target variable gets quantified by MI through its scores; higher mutual information scores show stronger relationships [19]. The Mutual relationship between X and Y is shown in equation 2.

$$I(X, Y) = \sum_{x \in X} \sum_{y \in Y} p(x,y) \log\left(\frac{P(x,y)}{p(x)p(y)}\right) \quad (2)$$

## 2.5 Recursive Feature Elimination (RFE)

RFE executes an iterative process that takes away the features which perform the least well according to model performance metrics. A model training process determines feature rankings by measuring how each feature affects the predictive capabilities of the model through RFE. The least important features are removed in each step while the model trains again with the available features. The process runs until it finds the best set of vital features [20]. Figure 5 shows the RFE Feature Elimination process.

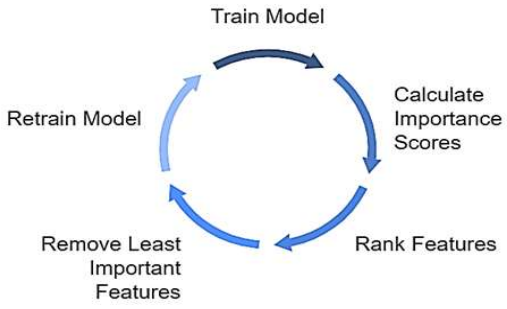


**Figure 5.** Recursive Feature Elimination Process

## 2.6 Proposed Model

A multitask model forms the basis of our approach to handle binary as well as multiclass classification operations. The model contains fully connected layers which utilize the ReLU activation function in every layer to enable it recognize complex data relationships. The neural network system accepts network features as input via the first layer which formats data for training purposes. The three sequential FC layers produce an output through 128 then 64 and finally 32 neurons while each uses ReLU activation processing. With this architecture the model successfully detects hidden patterns without getting limited by gradient disappearance. The program generates two distinct outputs through separate classification systems: first it uses sigmoid activation to detect "Normal" or "Attack" then employs softmax activation for multiclass attack recognition including Back, Ipsweep, Neptune, Nmap and other types. The integration of dropout layers between fully connected layers serves to prevent overfitting while achieving better generalization when dealing with new data. Figure 6 shows proposed model.

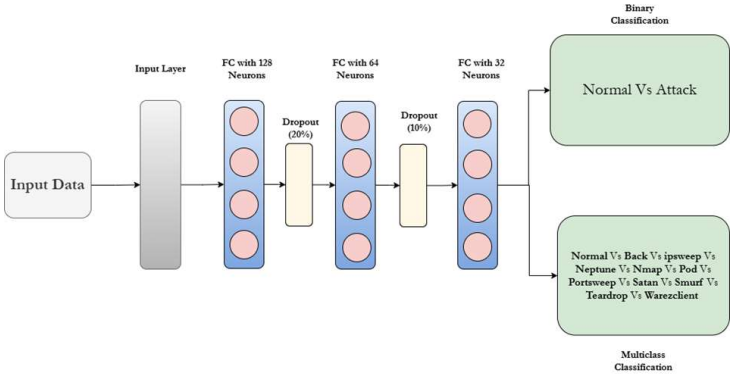


**Figure 6.** Proposed IntruDualNet Model

## 2.7 Model Compilation

The compilation uses Adam optimizer along with a learning rate value of 0.0001. Adam optimizer provides effective gradient handling along with automatic learning rate adjustment so it was selected for the application. Multiclass classification uses sparse categorical cross-entropy as its loss function since it operates well on integer labels. The standard loss mechanism for two-class classification is binary cross-entropy since it works with binary target outcomes of 1 and 0. The model assessment relies on accuracy as the main performance indicator suitable for binary and multiclass classification scenarios.

# 3. Result Analysis

## 3.1 Confusion Matrix

A confusion matrix is a tool used to evaluate the performance of a classification model by comparing the predicted labels with the actual labels. Figure 7 represents the confusion matrix for binary classification, where the model distinguishes between attack and normal instances. With an impressive accuracy of 99.70%, the model effectively identifies the two classes. The true positives (TP) show a large number of attack instances correctly classified as attacks (20,630), while the true negatives (TN) indicate a high number of normal instances correctly classified as normal (23,330). The model only misclassifies a few instances, with 16 attacks being falsely identified as normal (false positives) and 115

normal instances being incorrectly classified as attacks (false negatives). This demonstrates the model's ability to correctly detect cyberattacks while maintaining a strong performance in distinguishing normal network traffic.

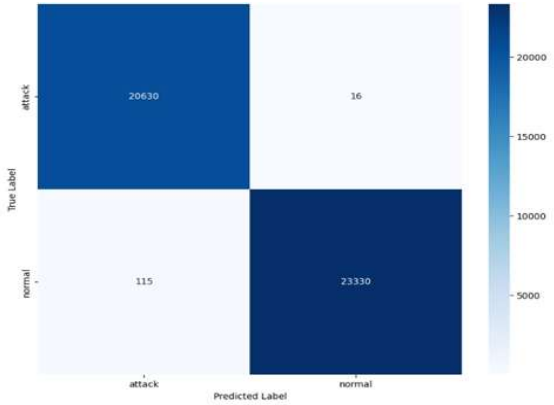


**Figure 7.** Confusion Matrix for Binary Classification

Figure 8 displays the confusion matrix for multiclass classification, where the model is tasked with identifying various attack types as well as normal traffic. The model achieves a high accuracy of 99.49%, effectively classifying different attack types, such as Neptune, with 14,424 true positives, and Normal, with 23,455 true positives. Other attack types, including Smurf, Portsweep, and Back, also demonstrate strong performance with minimal false positives and false negatives. Although there are a few misclassifications, such as Back with 333 false positives and Normal with 4 false negatives, the overall model performance remains robust. This confirms the model's reliability in accurately detecting a wide range of cyber threats.


**Figure 8.** Confusion Matrix for Multiclass Classification

## 3.2 Performance Evaluation

In this section The performance of the proposed model was evaluated using several standard evaluation metrics: accuracy, precision, recall, and AUC score. These metrics provide a comprehensive assessment of the model's performance, especially in the context of both binary and multiclass classification tasks.

**Accuracy**
Accuracy is the proportion of correct predictions (both true positives and true negatives) out of all predictions made by the model. It gives an overall sense of the model's performance. It is calculated as the proportion of accurate forecasts to all predictions

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{Total Instances}} \tag{3}$$

**Precision**
Precision measures the proportion of true positive instances among all instances predicted as positive. It indicates how many of the predicted positives are actually positive.

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \tag{4}$$

**Recall**
Recall measures the proportion of true positive instances among all actual positive instances. It shows how well the model identifies positive instances.

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \tag{5}$$

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

$$\text{F1 Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision+Recall}} \tag{6}$$

True Positives (TP) are the instances that the model correctly identifies as positive, meaning both the prediction and the actual condition are positive. True Negatives (TN) represent the instances that the model accurately predicts as negative, where both the prediction and actual condition are negative. Conversely, False Positives (FP) occur when the model incorrectly predicts a positive outcome for an instance that is actually negative, while False Negatives (FN) arise when the model mistakenly predicts a negative outcome for an instance that is actually positive.

**Table 1.** Neural network (binary classification) performance evaluation

| Metric | Class 0 | Class 1 | Macro Avg | Weighted Avg |
|---|---|---|---|---|
| Precision | 99% | 100% | 100% | 100% |
| Recall | 100% | 100% | 100% | 100% |
| F1-score | 100% | 100% | 100% | 100% |

Table 1 presents the performance of the neural network model in distinguishing between normal and attack instances. The model achieved 99.70% accuracy, with near-perfect precision, recall, and F1-scores, demonstrating its effectiveness in binary threat detection.

**Table 2.** Neural network (multiclass classification) performance evaluation

| Class | Precision | Recall | F1-score |
|---|---|---|---|
| Others | 89% | 54% | 67% |
| Back | 98% | 99% | 99% |
| Ipsweep | 96% | 98% | 97% |
| Neptune | 100% | 100% | 100% |
| Nmap | 94% | 98% | 96% |
| Normal | 100% | 100% | 100% |
| Pod | 100% | 97% | 99% |
| Portsweep | 99% | 99% | 99% |
| Satan | 99% | 98% | 98% |
| Smurf | 99% | 99% | 99% |
| Teardrop | 100% | 100% | 100% |
| Warezclient | 92% | 99% | 95% |

Table 2 illustrates the model's capability to classify multiple cyber threats, achieving 99.49% accuracy. The high precision and recall across different attack types highlight the model's robustness in detecting and categorizing cybersecurity threats.

**Table 3**. Comparison with previous work

| Ref No. | Method | Accuracy |
|---|---|---|
| [11] | ACAD-BMDL | 99.36% |
| [12] | Optimization-driven framework | 99.24% |
| [13] | CNN-LSTM | 98.55% |
| Proposed Model | IntruDualNet | 99.70% |

Table III compares the accuracy of different cyber threat detection methods. The Proposed method based on deep learning achieves the highest accuracy of 99.70%, outperforming previous methods such as ACAD-BMDL (99.36%), Optimization-driven framework (99.24%), and CNN-LSTM (98.55%). This highlights the superior performance of the proposed deep learning approach in accurately detecting cyber threats

# 4. Conclusion

The increasing capabilities of quantum computing present a major challenge to conventional cryptographic techniques, making the transition to post-quantum cryptography (PQC) imperative for ensuring long-term cybersecurity. This study analyzed the vulnerabilities of existing cryptographic systems and leveraged machine learning and deep learning models to enhance cyber threat detection. The research findings highlight the susceptibility of traditional encryption methods to quantum attacks and demonstrate the efficiency of AI-driven security approaches in mitigating cyber threats. The proposed neural network model achieved 99.70% accuracy in binary classification and 99.49% accuracy in multiclass classification, effectively identifying various attack types such as DDoS, SQL injection, and XSS. These results validate the potential of AI-based intrusion detection in strengthening cybersecurity defenses. Given the growing quantum threat landscape, the integration of PQC and AI-powered threat detection is critical for safeguarding sensitive digital assets. Future work should focus on refining hybrid security models and exploring real-time adaptive defense mechanisms to counteract emerging cyber risks in the quantum era.

# References

[1] Mahto, D., Khan, D., Yadav, D.: Security analysis of elliptic curve cryptography and RSA. 2016.
[2] Mavroeidis, V., Vishi, K., Zych, M., Jøsang, A.: The impact of quantum computing on present cryptography. In: ArXiv, abs/1804.00200, 2018.
[3] Muruganantham, B., Shamili, P., Kumar, S., Murugan, A.: Quantum cryptography for secured communication networks. Int. J. Electr. Comput. Eng., vol. 10, pp. 407–414 (2020).
[4] Bolfing, A.: Introduction to quantum computing. Cryptographic primitives in blockchain technology. 2020.
[5] Mamatha, G., Dimri, N., Sinha, R.: Post-quantum cryptography: Securing digital communication in the quantum era. ArXiv, abs/2403.11741, 2024.
[6] Hasan, N., et al.: Brain tumor diagnosis using a hybrid method of BoVW, LBP, and neural networks. In: 2024 IEEE 3rd International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON), Dhaka, Bangladesh: IEEE, Nov. 2024, pp. 264–269.
[7] Althobaiti, O., Dohler, M.: Cybersecurity challenges associated with the Internet of Things in a post-quantum world. IEEE Access, vol. 8, pp. 157356–157381 (2020).
[8] Hasan, N., et al.: Epileptic seizure prediction using a deep hybrid CNN-GAN model on EEG data. In: 2024 IEEE 3rd International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON), Dhaka, Bangladesh: IEEE, Nov. 2024, pp. 270–275.
[9] Gupta, R., Tanwar, S., Tyagi, S., Kumar, N.: Machine learning models for secure data analytics: A taxonomy and threat model. Comput. Commun., vol. 153, pp. 406–440 (2020).
[10] Hasan, N., Ahmed, M. F.: Wearable technology for elderly care: Integrating health monitoring and emergency alerts. Journal of Computer Networks and Communications, vol. 2024, no. 1, p. 5593708, Jan. 2024.
[11] Al Mazroa, A., Albogamy, F. R., Ishak, M. K., Mostafa, S. M.: Boosting cyberattack detection using binary metaheuristics with deep learning on cyber-physical system environment. IEEE Access, vol. 1 (2025).
[12] Batchu, R. K., Bikku, T., Thota, S., Seetha, H., Ayoade, A. A.: A novel optimization-driven deep learning framework for the detection of DDoS attacks. Dental Science Reports, vol. 14, no. 1 (2024).
[13] Imran, M., Malik, K. R., Almogren, A., Malik, T. S., Khan, A. H., Tanveer, J., Rehman, A. U.: Enhancing intrusion detection: A hybrid machine and deep learning approach. J. Cloud Comput., vol. 13, no. 1 (2024).
[14] Hasan, N., Ahmed, M. F., Nasif, M. A., Haq, Md. R., Rahman, M.: Hybrid feature extraction approach for robust brain tumor classification: HOG, GLCM, and artificial neural network. In: 2024 6th International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT), Dhaka, Bangladesh: IEEE, May 2024, pp. 1292–1297.
[15] Aliero, M., Ghani, I., Qureshi, K., Rohani, M.: An algorithm for detecting SQL injection vulnerability using black-box testing. J. Ambient Intell. Humanized Comput., vol. 11, pp. 249–266 (2019).

[16] Hasan, N., et al.: Lung cancer classification using CNN and random forest. In: 2024 IEEE 3rd International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON), Dhaka, Bangladesh: IEEE, Nov. 2024, pp. 276–281.

[17] En, V., Selvarajah, V.: Cross-Site Scripting (XSS). In: 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), pp. 1–5, 2022.

[18] Hayat, T., Islam, M. S., Hossain, M., Hasan, N., Parvez, M., Hoque, Md. J.: Machine learning techniques for brain tumor classification: A CNN-SVM approach. In: 2024 International Conference on Innovations in Science, Engineering and Technology (ICISET), Chittagong, Bangladesh: IEEE, Oct. 2024, pp. 1–6.

[19] Nguyen, X., Zhou, S., Chan, J., Bailey, J.: Can high-order dependencies improve mutual information-based feature selection? Pattern Recognit., vol. 53, pp. 46–58 (2016).

[20] Demir, S., Şahin, E.: Assessment of feature selection for liquefaction prediction based on recursive feature elimination. Eur. J. Sci. Technol., vol. 2021.