NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Special Issue – 1, 2024
E – ISSN – 2583-7559

Quantum Machine Learning Based Network IDS for DDoS Attack Detection in IoT: A Novel Approach

Bikram Bikash Das
Woxsen University, Hyderabad
Department of Computer Science,
School of Sciences
Kamkole, Sadasivpet, Sangareddy District, Hyderabad, India

***Abstract*— A Hybrid Classical Quantum Machine Learning (QML) Model for Mitigating and identifying Distributed Denial of Service (DDoS) Detection is a cutting-edge approach that combines classical machine learning techniques with quantum computing to enhance the performance of detecting such attack with more efficiently and precise accuracy rate with reduced false positive. The primacy concern for this paper is to investigate some of the current research challenges for mitigating Distributed Denial of Service (DDoS) for IoT based network. It becomes very difficult to identify the signature of such attack due to the huge volume of user request traffic for the target machine [1] .This Paper has outlined the detection of Distributed Denial of Service attack that can be performed by Quantum computer along with the Machine Learning techniques and also provided study of various existing research for the same. This paper also proposed a Hybrid Classical Quantum Machine learning Model for mitigating with such attack for future.**

***Keywords*— Quantum Computing, DDoS Attack, Quantum Machine Learning (QML), IoT, Intrusion Detection Systems (IDS).**

I. INTRODUCTION

Quantum computing uses the concepts of Quantum Mechanics like Superposition and Entanglement and implements with Quantum Bits or Qubits rather than 0's and 1's or classical Bits and it uses the principles of quantum mechanics to perform certain types of calculations significantly faster than classical computers. [3] In the context of DDoS detection, various network traffic features can be extracted from incoming data packets. Classical machine learning methods can be used to perform the initial data preprocessing.
Mitigating with DDoS attacks continue to pose a significant threat to online services and networks. Traditional methods of DDoS detection often struggle to keep pace with evolving attack techniques. In recent years, quantum computing has emerged as a promising technology with the potential to revolutionize the field of machine learning. [5] This paper presents a systematic study of the challenges and research opportunities in applying hybrid classical-quantum machine learning techniques to enhance DDoS detection.

We explore the integration of classical machine learning models with quantum algorithms and hardware, aiming to faster processing with reduced false positive rates with accurate predictions and to detect of DDoS attack more efficiently than the traditional machine. This study provides insights into the current state of research for mitigating DDoS attack for IoT using Quantum Machine Learning that combines the traditional machine learning algorithm to be processed with Quantum Computing methodologies, identifies key challenges and suggests promising directions for future work in this critical area of cybersecurity.

II. Related Work:

Distributed Denial of Service (DDoS) attacks represent a persistent and evolving threat to network and online service availability. Traditional DDoS detection methods often face challenges in keeping pace with the complexity and scale of these attacks. [9] Quantum computing and quantum machine learning (QML) have emerged as promising technologies with the ability to perform more efficiently and to enhance the accuracy of DDoS detection. Hybrid Quantum computing is the preferred industry term where a quantum computer and a classical computer working together to solve a Problem.

Previous Research on DDoS attack detection has identified that the effectiveness of methodology that has been used by considering traditional ML Algorithm and taking immediate actions for DDoS attack [1]

III. Intrusion Detection System (IDS) for DDoS Detection

Intrusion detection systems (IDS) are classified into two categories. First is NIDS meaning those IDS system that are monitoring any deviations or abnormal behavior in the whole

Network consisting of different hosts and secondly HIDS where the IDS work only within a particular Machine or Host.

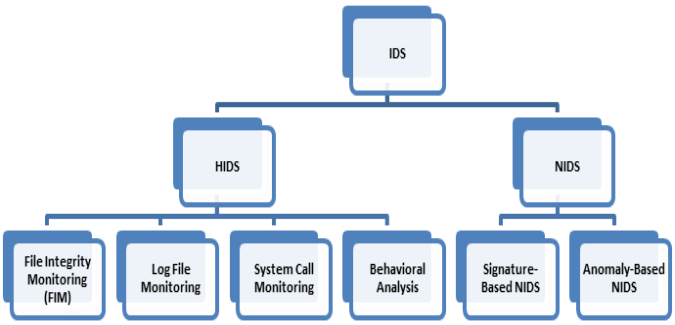


Figure: Types of Intrusion Detection System (IDS)

3.1 HIDS Vs NIDS

The IDS systems are security solution in that is used to identify any abnormal behavior in the Network and hosts and detect any malicious behavior within a network.

HIDS primarily focuses on analyzing the whole network for any deviations then the normal traffic and events occurring on individual machines that exceeds certain threshold value. It provides visibility into host-level events, processes, file modifications, and other activities that may indicate unauthorized access or malicious behavior. Here are some common types of HIDS:

I. File Integrity Monitoring (FIM): FIM focuses on monitoring and detecting unauthorized changes to critical system files, configurations, or directories. It maintains a database of file signatures or checksums and compares them periodically to detect any modifications or tampering.

II. Log File Monitoring: HIDS analyzes log files generated by the operating system, applications, or services running on the host. It looks for patterns or events indicative of security breaches, such as multiple failed login attempts, privilege escalation attempts, or unusual system activity.

III. System Call Monitoring: HIDS monitors system calls made by applications or processes running on the host. It compares the system calls against a known set of malicious or unauthorized actions, generating alerts if suspicious behavior is detected.

IV. Behavioral Analysis: Some HIDS solutions use behavioral analysis methodologies to identify normal traffic and detect any malicious behavior in the network. These systems look for abnormal activity, such as unexpected network connections, unusual process behavior, or unauthorized privilege escalation attempts.

NIDS as the name itself conforms that it generally works at the network level for network traffic analysis in order to examine suspicious packets of data flowing through the network. Here are two common approaches to NIDS:

I. **Signature-based:** It generally works with some previously encountered attack signatures that are compared against the network traffic to classify them as either normal or malicious. If there is any match of the generated patterns with the known signatures, it will intimate the network administrator in the form of alerts. The primary disadvantage is that it cannot identify any novel or unknown attacks.

II. **Anomaly-based**: this basically utilizes the statistical analysis and Machine Learning algorithms to identify abnormal patterns, such as unusual traffic volumes, protocols or connection attempts. Anomaly-based NIDS can detect unknown attacks or variations of known attacks, but it may also produce false positives.

Both NIDS and HIDS are important components of a comprehensive intrusion detection and prevention strategy. They complement each other by providing visibility into different aspects of the network and host environments, allowing organizations to detect and respond to security incidents effectively.

IV. Related Work:

Traditional Machine Learning model for Intrusion Detection may produce accurate results by utilizing long time but results in poor accuracy for quick training when the velocity and volume of data increases. Hence Fast and efficient Network Intrusion Detection is utmost importance in order to overcome the barriers with the traditional Machine Learning based IDS System. [8]

Ref	**Analysis of Existing Literature**		
	Attack types, dataset, techniques used	***Advantage***	***Drawbacks***
[5]	IoT heterogeneous perceptual network, Game	Detects multiple network	Can results Large number of false

Ref	Analysis of Existing Literature		
	Attack types, dataset, techniques used	***Advantage***	***Drawbacks***
	theory, by applying modified particle swarm optimization, clustering algorithm called ULEACH	attacks with reduced energy consumption	positives.
[2]	Malicious attacks on Private Hospital network, A hybrid classicalquantum neural network, KDD99 dataset.	Easy to train the model by utilizing the Quantum Assisted Activation Function.	Produces false positives, more complex while increasing the size of qubits.
[9]	Adaptive IDS & IPS is proposed for IoT, utilizes the IoT network traffic for encoding and decodes the network traffic data for further analysis.	Ability to cope up huge volume of network devices with more Enhance security.	Results Large number of false positives.
[10]	The QSVM and Quantum Convolution Neural Network (QCNN), Stream dataset is used for the quantum classifiers	More Accurate results using Quantum ML-based Intrusion detection for Big Data Analysis.	IoT Growth results more false Positives where QCNN provides more accuracy as compared with Quantum Support Vector Machine.
[11]	Decision tree classifier,Used Aegean Wi-Fi Intrusion Dataset also known as AWID Dataset	Constant removal is efficient along with recursive feature elimination	IoT Growth can result less promising results.
[12]	IoT based Sensor Dataset, Uses Signature based IDS to classify both known and previously	Inspects network activity traffic data streams to detect and	Identify only Known Patterns as benign and malicious that was previously encountered.
	Unknown attacks, A novel string coordinating strategy algorithm is utilized.	identify misuse instances that are misused to perform intrusion.	
[13]	Attacks on IoMT which is Internet of Medical Things data, utilizing Elliptic Curve Cryptography(ECC)	More Efficient Data Integrity that requires very less parameters, Size of Encryption keys to be minimal.	Used only symmetric encryption and has not provided comparative analysis for using symmetric over the asymmetric encryption.
[14]	DoS attack dataset, UNSW-NB15 dataset, ML-supervised algorithm-based IDS for IoT (ML-IDS), dimensionality reduction Using Principal Component Analysis (PCA).	Perform more efficiently for identifying malicious activity using different ML algorithm, utilizes the methods for Feature Dimensionality reduction.	Not suitable for novel dataset. More sophisticated IDS can be enhanced using Deep Learning techniques that are suitable for the IoT environment

Classical Machine Learning: In a hybrid model, classical machine learning algorithms can also be integrated. After the quantum processing step, classical machine learning algorithms can further refine the model's predictions. Ensemble techniques, such as stacking, may be employed to combine classical and quantum models.

Real-time Monitoring: The hybrid model is applied to real-time network traffic data. [8] It continuously monitors incoming data packets and makes predictions regarding whether they represent a DDoS attack or legitimate traffic.

Feedback Loop: The model can incorporate a feedback loop to continuously adapt and improve its detection capabilities based on new data. [6] This adaptive learning approach is critical for effectively countering evolving DDoS attack techniques.

Alert and Mitigation: When the model detects a DDoS attack, it can trigger an alert and initiate countermeasures to mitigate the attack, such as traffic filtering, rerouting, or rate limiting.

The advantage our proposed model is its potential to handle and monitor Big IoT network complex traffic often associated with DDoS detection more efficiently than classical machine learning models alone. Additionally, the adoption of such models may be limited by the availability of quantum hardware and the need for expertise in both classical and quantum computing.

Detection of such attacks in an Internet of Things (IoT) network infrastructure is a complex and crucial task due to the scale, diversity and resource constraints of IoT devices. A hybrid machine learning approach can enhance DDoS detection in IoT networks by combining multiple techniques to improve accuracy and robustness.

V. DDoS attacks affecting IoT Networks

Malicious activity in order to disrupt the normal operation of IoT devices and services by overwhelming with a massive volume of traffic is a major concern. The following section describes the overview of DDoS attacks along with some techniques and strategies to mitigate those attacks.

5.1 IoT Devices as Attack Vectors: In an IoT network, devices often have limited processing power and bandwidth. Attackers can compromise these devices and turn them into bots, forming a botnet. These botnets can be used to launch DDoS attacks.

5.2. Attack Types: IoT DDoS attacks can take various forms, including: Traffic Floods: Overloading the network with excessive traffic, exhausting bandwidth and resources.

5.3. Protocol-Based Attacks: Targeting specific IoT communication protocols, exploiting vulnerabilities or overwhelming them.

5.4. Application Layer Attacks: Attacking IoT application servers, such as web servers or MQTT brokers, with HTTP floods or CoAP message floods. There is a need to exploiting DNS servers to amplify the volume of attack traffic.

5.5. Attack Impact: DDoS attacks on IoT networks can have severe consequences, including: Disruption of IoT services, making them unavailable to users. There will be financial losses due to downtime and service interruptions and Reputation damage for service providers. There may be possibility of data breaches or unauthorized access to IoT devices.

5.6. Mitigation Strategies: To protect IoT networks from DDoS attacks, consider the following strategies:

5.7. Traffic Monitoring and Anomaly Detection: In order to protect IoT networks from DDoS attacks, it is necessary to continuously monitor the network traffic in order to find any abnormal patterns and to detect those unusual patterns. Machine Learning or rule-based systems can be used to identify anomalies in network traffic, allowing for early detection of those attacks.

5.8. Rate Limiting: Rate limiting on IoT devices can be used to prevent excessive traffic from reaching them.

5.9. Traffic Filtering: Traffic filtering and Access Control Lists (ACLs) can be employed to block malicious traffic at the network perimeter. Content Delivery Networks (CDNs) is more generally used to distribute traffic and absorb DDoS attacks, reducing the load on IoT devices.

Other factors for DDoS attacks affecting IoT Networks are discussed below:

IoT Device Security: Ensure that IoT devices are properly secured, regularly patched, and have strong, unique credentials to prevent compromise and botnet formation.

Load Balancing: Implement load balancing to distribute traffic evenly across multiple IoT servers, preventing any single device from being overwhelmed.

DDoS attacks affecting IoT Networks: Consider subscribing to DDoS mitigation services provided by specialized vendors that can scrub incoming traffic and filter out malicious requests.[10]

Behavioral Analysis: Employ behavioral analysis techniques to detect deviations in the behavior of IoT devices, as attackers may attempt to exploit vulnerabilities or execute unauthorized actions.

DDoS attacks are an ongoing threat to IoT networks, and their impact can be significant. Implementing a multi-layered defense strategy and staying proactive in monitoring and securing IoT devices are essential steps to minimize the risk and impact of these attacks.

VI. Hybrid approach for DDoS detection in IoT networks

Here's a high-level overview of a hybrid approach for DDoS detection in IoT networks:

6.1 Data Collection and Preprocessing: Collect network traffic data from IoT devices, such as packet headers, flow data, and device behavior logs. Preprocess the data to remove noise and irrelevant information, and extract relevant features.

6.2 Feature Selection: Utilize feature selection techniques to identify the most relevant features for DDoS detection. Feature selection helps reduce dimensionality and improves model performance.

6.3 Ensemble Learning: Combine the results from both unsupervised and supervised models using ensemble techniques like stacking or voting. This can improve detection accuracy by leveraging the strengths of different models.

6.4 Monitoring IoT Network Data in Real time: continuously analyze the IoT Network Traffic data for DDoS attack detection immediately in Real time or as they occur.
6.5 Thresholding and Alarms: Set appropriate thresholds for anomaly detection and generate alarms or alerts when suspicious activity is detected. Thresholds can be dynamic and adapt to the network's baseline behavior.

6.6 Feedback Loop: Create a feedback loop that updates the model with new data and adapts to changing attack techniques and network conditions. Continuous learning is crucial to maintaining detection accuracy.

6.7 Historical Data Analysis: Analyze historical data to identify recurrent attack patterns and refine the detection models accordingly.

6.8 Behavioral Analysis: Incorporate behavioral analysis techniques to detect deviations in IoT device behavior, as DDoS attacks often involve compromised devices behaving abnormally. Anomaly Correlation is used to correlate anomalies across multiple IoT devices and network segments to identify coordinated DDoS attacks.

6.9 Resource Management: Optimize resource usage, especially in resource-constrained IoT devices, by implementing lightweight machine learning models or offloading computation to edge devices or cloud servers.

6.10 Traffic Filtering and Mitigation: Implement traffic filtering and mitigation strategies to block or redirect malicious traffic away from the network. Finally testing and Evaluation continuously evaluate the performance of the hybrid DDoS detection system using historical data and simulated attacks to ensure its effectiveness.

6.11 Regulatory Compliance: Ensuring that the hybrid DDoS detection system complies with relevant regulations, especially in cases where IoT devices handle sensitive data.

Quantum Computing: Block Sphere

A Bloch Sphere is the state space of all possible points to which a state vector can point to. A sample python code for Plotting the Bloch Sphere is as follows:

```
# To get the eigenvector you should use the state vector simulator in the core of the circuit (without measurements)

backend = Aer.get_backend('statevector_simulator')

# Execute the circuit result = execute(qc_y, backend).result().get_statevector(qc_y, decimals=3)

# Printing the state after Y gate
print("\nQuantum state is:",result)

# Plotting the Bloch Sphere
plot_bloch_multivector(result)
```

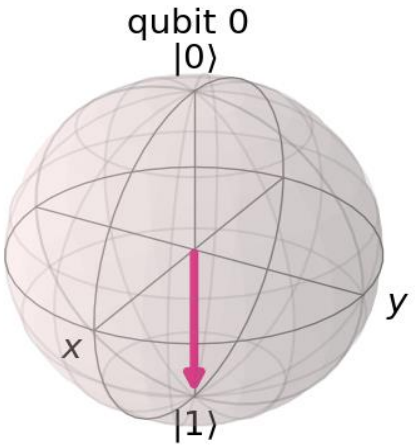
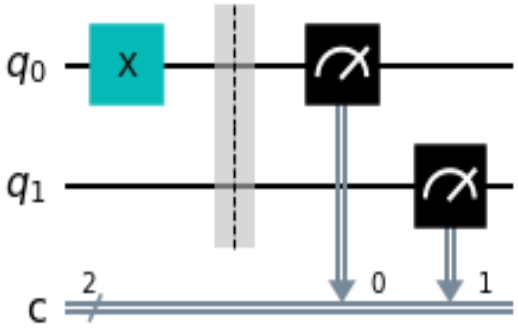


Figure: Quantum Bloch Sphere of two qubits

Example of Quantum Gate:

```
# X-gate on a |0> qubit and measurement with quantum circuit
qc_x = QuantumCircuit(2,2,name="qc") #Quantum Circuit
qc_x.x(0) # X Gate on 1st Qubit
qc_x.barrier()
qc_x.measure(0,0)
qc_x.measure(1,1)
#qc.measure([0,1], [0,1])
qc_x.draw('mpl')
```

The measurement of the two qubits using the Quantum X gate on the First Qubits is as follows:



Two Qubit Measurements

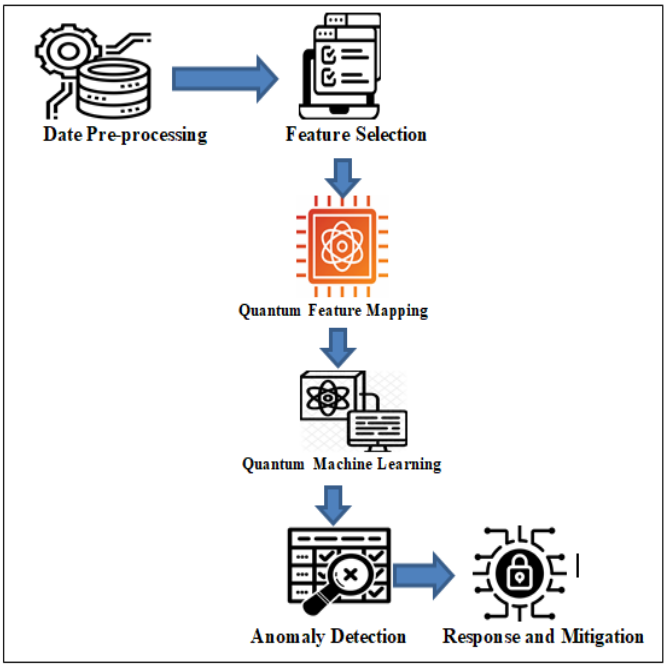


Figure: The Proposed Hybrid Classical Quantum Machine Learning Framework

VII. Anomaly Based Machine Learning algorithm for DDoS Attack detection

An anomaly-based ML algorithm involves identifying abnormal patterns of network traffic that may indicate an ongoing attack in the IoT Network [8]. Here are some machine learning algorithms commonly used for anomaly-based DDoS attack detection in IoT networks:

7.1 Isolation Forest: Isolation Forest is effective at isolating anomalies from the majority of normal traffic. It's a tree-based algorithm that measures how quickly data points are isolated from others in the dataset. Anomalies are isolated faster.

7.2 One-Class SVM: It can be effectively used for the analysis of normal traffic data and identifies deviations as anomalies and one class SVM (Support Vector Machine) is considered as Supervised ML technique. It's especially useful when you have limited labeled attack data.

7.3 Autoencoders: Autoencoders are neural networks trained to reconstruct input data. Anomalies are detected by measuring the reconstruction error; larger errors indicate anomalies. Variational Autoencoders (VAEs) can also be used.

7.4 Principal Component Analysis: It can be used for anomaly detection and is considered as a dimensionality reduction methodology by comparing the reconstruction error of data points after projecting them onto a lower-dimensional subspace.

7.5 K-Means: This method can be useful and works efficiently for grouping network traffic data such as IoT network data generated by different sensors and making them converted into different clusters.

7.6 Density-Based Spatial Clustering of Applications with Noise):
It identifies the anomalies or any deviations in the IoT network traffic data that are not fitted into any of the clusters are considered as noise. It is also considered as density based clustering technique or DBSCAN clustering algorithm in short.

7.7 Random Forests: Random Forests can be used for anomaly detection by training an ensemble of decision trees on network traffic data. Data points that are not well-explained by the ensemble may be anomalies.

7.8 HMM (Hidden Markov Models): HMMs model the sequential nature of network traffic. Anomalies can be detected by observing transitions between states that have low probabilities.

7.9 Long Short-Term Memory Networks: This can be utilized for modeling sequential data, which is common in IoT network traffic. Anomalies can be detected based on deviations from expected temporal patterns.

7.10 GANs (Generative Adversarial Networks): GANs can generate synthetic normal network traffic data. Anomalies can

be detected by identifying data points that deviate significantly from the generated data.

VIII. Conclusion:

By using simulated or real-world IoT devices and networks, researchers can test the performance of quantum machine learning algorithms in detecting and preventing various types of cyberattacks, malware infections and data breaches. This can involve generating simulated attack scenarios or testing the algorithms on real-world data from past attacks.

Overall, the combination of simulated or real-world IoT devices and networks, and quantum machine learning algorithms, can provide a powerful tool for improving the security of IoT network and preventing various kinds of cyberattacks. Additionally, continuous monitoring and retraining are essential to adapt to evolving attack techniques and network conditions.

REFERENCES

1. Li, L., Zhou, J., Xiao, N. (2007). DDoS Attack Detection Algorithms Based on Entropy Computing. In: Qing, S., Imai, H., Wang, G. (eds) Information and Communications Security. ICICS 2007. Lecture Notes in Computer Science, vol 4861. Springer, Berlin, Heidelberg.

2. N. Laxminarayana, N. Mishra, P. Tiwari, S. Garg, B. K. Behera and A. Farouk, "Quantum-Assisted Activation for Supervised Learning in Healthcare-based Intrusion Detection Systems," in IEEE Transactions on Artificial Intelligence, 2022, doi: 10.1109/TAI.2022.3187676.

3. Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices, M. Eskandari, Z. H. Janjua, M. Vecchio and F. Antonelli, "Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices," in *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6882-6897, Aug. 2020, doi: 10.1109/JIOT.2020.2970501.

4. S. F. Ahmad, M. Y. Ferjani and K. Kasliwal, "Enhancing Security in the Industrial IoT Sector using Quantum Computing," *2021 28th IEEE International Conference on Electronics, Circuits, and Systems (ICECS)*, Dubai, United Arab Emirates, 2021, pp. 1-5, doi: 10.1109/ICECS53924.2021.9665527

5. A. Kjamilji, A. Levi, E. Savaş and O. B. Güney, "Secure Matrix Operations for Machine Learning Classifications Over Encrypted Data in Post Quantum Industrial IoT," 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 2021, pp. 1-8, doi: 10.1109/ISNCC52172.2021.9615794.

6. D. T. Uysal, P. D. Yoo and K. Taha, "Data-Driven Malware Detection for 6G Networks: A Survey From the Perspective of Continuous Learning and Explainability via Visualisation," in IEEE Open Journal of Vehicular Technology, vol. 4, pp. 61-71, 2023, doi: 10.1109/OJVT.2022.3219898.

7. R. A. Sadek and H. M. Elbadawy, "Towards IoT Era with current and Future Wireless Communication Technologies: An Overview," 2022 39th National Radio Science Conference (NRSC), Cairo, Egypt, 2022, pp. 343-353, doi: 10.1109/NRSC57219.2022.9971196.

8. Alexei Petrenko, "3 Development of Quantum Cryptanalysis Algorithms," in Applied Quantum Cryptanalysis , River Publishers, 2022, pp.97-128.

9. H. A. Al-Mohammed et al., "Machine Learning Techniques for Detecting Attackers During Quantum Key Distribution in IoT Networks With Application to Railway Scenarios," in IEEE Access, vol. 9, pp. 136994-137004, 2021

10. Bakhsh, Sheikh & Alghamdi, Saleh & Alsemmeari, Rayan & Hassan, Raheel. (2019). An adaptive intrusion detection and prevention system for Internet of Things. International Journal of Distributed Sensor Networks. 15. 155014771988810. 10.1177/1550147719888109.

11. Kalinin, M., Krundyshev, V. Security intrusion detection using quantum machine learning techniques. *J Comput Virol Hack Tech* 19, 125–136 (2023). https://doi.org/10.1007/s11416-022-00435-0

12. Tarek Gaber, Amir El-Ghamry, Aboul Ella Hassanien, Injection attack detection using machine learning for smart IoT applications, Physical Communication, Volume 52,2022, 101685, ISSN 1874-4907,https://doi.org/10.1016/j.phycom.2022.101685. (https://www.sciencedirect.com/science/article/pii/S1874490722000490)

13. Ajay Kumar, K. Abhishek, M.R. Ghalib, A. Shankar, X. Cheng, Intrusion detection and prevention system for an IoT environment, Digital Communications and Networks, Volume 8, Issue 4, 2022, Pages 540-551, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2022.05.027.(https://www.sciencedirect.com/science/article/pii/S2352864822001201)

14. Sangjukta Das, Suyel Namasudra, A Novel Hybrid Encryption Method to Secure Healthcare Data in IoT-enabled Healthcare Infrastructure, Computers and Electrical Engineering, Volume 101, 2022, 107991, ISSN 0045-7906,

15. Saheed, Yakub & Abiodun, Aremu & Misra, Sanjay & Holone, Monica & Colomo-Palacios, Ricardo. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal. 61. 9395-9409. 10.1016/j.aej.2022.02.063.