Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 10, 2025

DETECTION OF IOT-BASED CYBER ATTACKS USING MACHINE LEARNING TECHNIQUES

Zartasha Kiran[1], Awais Rasool[*2], Kainat Shahid[3], Nimra Razzaq[4]

[1,*2]*Department of Software Engineering The University of Lahore*
[3]*Department of Information Technology Government College University Faisalabad*
[4]*Department of Computer Science University of Agriculture Faisalabad*

[1]zartasha.kiran@se.uol.edu.pk, [*2]awais.rasool@se.uol.edu.pk, [3]kainatshahid528@gmail.com, [4]csnimra@gmail.com

DOI: https://doi.org/10.5281/zenodo.17414455

Keywords
Internet of Things (IoT), Cybersecurity, Machine Learning, Intrusion Detection, KDD99-IoT Dataset

Article History
Received: 28 August 2025
Accepted: 07 October 2025
Published: 20 October 2025

Corresponding Author: * Awais Rasool

Abstract
The Internet brings Things together a huge number of gadgets that can communicate with one another with minimal user intervention. IoT devices are progressively deployed day-by-day life. Many of these devices are vulnerable due to insecurity, execution, and design. Cyber-attacks are currently posing a significant threat to IoT security. These risks have the potential to steal sensitive information, resulting in financial and reputational harm. IoT devices can now stay connected for longer periods without the need for human interaction. This necessitates the development of intelligent network-based security solutions, such as machine learning systems. Although several studies have examined the utilization of Machine Learning arrangements in attack discovery issues in recent years. The desire to add the field by assessing various ML methods that utilized to distinguish IoT network attacks fast and effectively in this study. A unique dataset, KDD99-IoT, is utilized to assess different discovery calculations. This dataset consists of four types of attacks DoS, Probe, U2L and U2R. In the execution stage, diverse AI calculations are used and the greater part of them accomplished superior. New provisions were removed from the KDD-IoT dataset throughout the execution and contrasted and concentrate the writing, and the new elements provided improved outcomes. In this research the three algorithms were used to detect Cyber-attacks. KNN, Logistic Regression and K-Means Clustering were used, all of these algorithms the Logistic Regression Provide best result 98% accuracy and KNN 97% accuracy. K-mean algorithm are used to make Clusters of the Attacks.

1. INTRODUCTION

Worries over security and protection in regards to PC networks are expanding on the planet, and PC security has turned into a prerequisite because of the spread of data innovation in day-to-day existence. AI approaches have been utilized for various organization security errands, for example, network traffic investigation interruption identification and botnet location. The use of AI in the detection of assaults is becoming a hot topic, and machine learning (ML) is increasingly being applied in network security applications. The work comprises of the way that the discovery of malware dangers are the primary difficulties in the field of network safety utilizing IoT-based framework. Malware assaults are high dangers to think twice about the security of IoT. There is a risk that important data could be stolen, causing

significant monetary and reputational damage[1]. To do as such, will assess an assortment of AI methods that will be utilized to rapidly and successfully recognize IoT system attacks. Attacks in this dataset fall into Four crucial characterizations: Probe, DoS, U2L and U2R[2].

The ability of an IoT setup to automate a condition or action that is based on data is seen as critical, and machine learning calculations are used in projects such as relapse prevention and to extract useful information from data provided by devices or by individuals. Two primary types of digital examination can be used in an IoT organization: signature-based and peculiarity-based. According to Mark Based Procedures, assaults can be identified by identifying specific traffic qualities (also referred to as "marking"). These strategies have a few advantages in properly identifying all known assaults without issuing a large number of false cautions."). Some fictional works employ signature-based systems to identify assaults [3].

1.1 Cyber Attack

Malware is a term that refers to malicious software such as spyware, ransomware, viruses, and worms, among other types of threats. Malware infiltrates a network by taking advantage of a vulnerability, which is often established when a user clicks on a potentially hazardous link or email attachment, which then installs possibly lethal software on the system. Once malware has gained access to a computer system, it may do the following actions Access to critical network components is denied (ransomware) Installs potentially harmful software, such as to collect information discreetly, viruses transfer data from the hard disc in the background (spyware). As a result, the system is rendered inoperable. A cyber-attack is an operation that is designed to change, erase, or steal data from a computer or any component of a computerized information system, as well as to exploit or damage a network[4]. It is also known as a cyber incident. As commercial digitalization has gained popularity over the last several years, cyber-attacks have increased in frequency and frequency of occurrence. One thing is for sure: There are many distinct kinds of assaults. The Most Common Types of Cyber Attacks

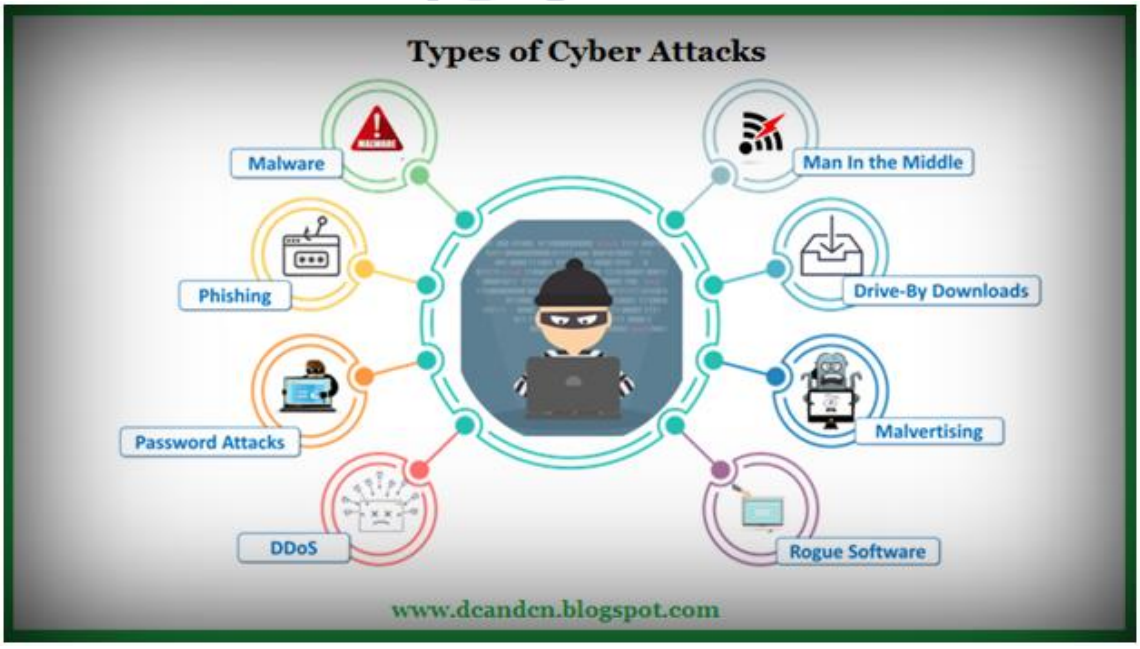

Figure 1: Cyber Attacks types

1.2 Internet of things (IOT)

The Internet of Things is a place where real, moving "Things" can connect with each other. They are

implanted with electronic chips, sensors, and other types of equipment. It's not hard to find the names of Radio Frequency IDs all over the place [5].

Web of Things (IoT) empowers combination and executions between this present reality protests independent of their geological areas. Organizational security and insurance processes are of utmost importance and challenge in this environment. The wellbeing proportions of IoT gadgets rely on the size and sort of association wherein it is forced. The conduct of clients powers the security entryways to participate. At the end of the day, can say that the area, nature, utilization of IoT gadgets choose the safety efforts [6].

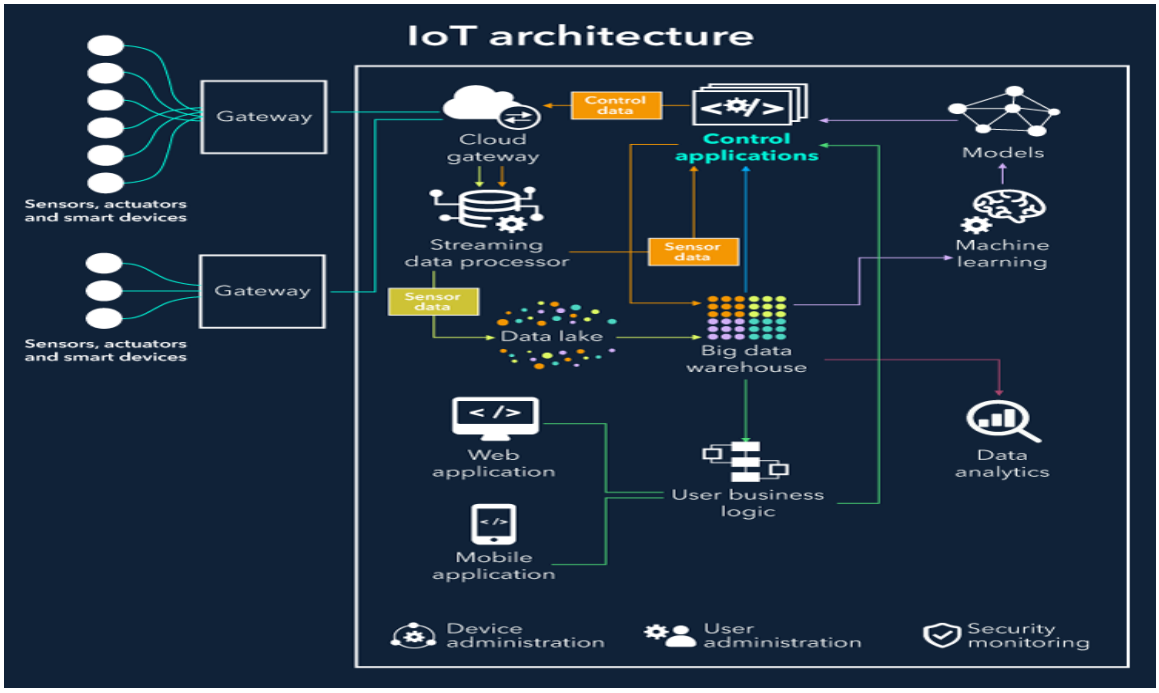

Figure 2: Internet of Thing

This work consists of the fact that the detection of malware threats are the main challenges in the field of cybersecurity using IoT-based system. Malware attacks are high risks to compromise the security of IoT. These threats may steal important information that causes economic and reputational damages. In this research we will solve this problem comparing and contrasting several machine learning techniques that may be utilized to swiftly and efficiently identify IoT network intrusions is being undertaken. During the experiment, Couple of machine learning algorithms will be implemented in the KDD 99 dataset[7].

2. REVIEW OF LITERATURE

Many examinations have shown that AI methods can be applied to help assault location undertakings, including k-implies, counterfeit neural organizations, notwithstanding Random Forest, auto-encoder, and others, a couple of makers have applied unassisted to their work AI computations for distinguishing proof issues. Auto-encoders are presumably the principle autonomous calculations that have been utilized in different works; for instance,

Sciences (2015) recognized that the availability of Security in information and communication systems is very important when it comes to the integrity and confidentiality of information and services, as well as the availability of these things from the beginning of the development of global communication networks, there have been activities aimed at preventing people from being able to communicate with each other. These activities require the development of new ways to protect against them. The Internet of Things (IoT)

concept is a big problem because it will make a lot more things connected. It is possible to use that kind of environment to make DDoS attacks. DDoS attacks get more and more common when there are more connected devices in the IoT concept. It doesn't matter how new methods to guard against DDoS assaults are being investigated since new ways to protect against new sorts of attacks produced by changes in the world and new communication technologies are continuously being researched.

Dusha *et al.*(2018) designed that is what the taxonomy, summaries, and organization of recent research on intrusion detection systems in IoT that was found out about by reading the research is explained in this way: It's possible to see the security holes that arise from the information exchange technologies used in the Internet of Things through this study. They can also learn about different security attacks and how to fight them. In this paper, mostly talked about IDS research efforts for the Internet of Things 20 papers were chosen for the literature. They talk about the IDS taxonomy, problems, and ways to protect against security attacks[10]. Some of these papers were written between 2014 and 2017. The different types of attacks are talked about, as well as ways to deal with them. IDS and IoT are two things that this work is used for. It helps researchers who work in IDS understand what these things are. It is important to know what kind of attack there is and who did it. A sensor node that doesn't have a lot of space and can detect wormhole attacks of two types of packet relay and encapsulation. Attack detection rates are better than they were with previous methods[11].

Kalash *et al.*(2018) presented that everything else being equal, they used both old and new parts of their system that had been unused since malware trials to make a malware classifier and called their system OPEM. They utilized recurrence of the event of functional codes as static elements while execution hints of executable documents, framework calls, exemptions as powerful components to prepare their order model. The outcomes showed that the half and half methodology perform much improved as a united approach as opposed to the successively of motionless and active strategies independently. Various assessments have been guided for the depiction of malware parts to work on the demonstration of assortment results also as a reducing on schedule, scope, and source above. Used, for instance, presented a CNN and picture-based malware grouping technique. Their model accomplished 70.52% exactness. They arbitrarily isolated just 10% examples in a family for testing[13].

Roopak *et al.*(2019) recognized many Internets of Things (IoT) networks have been targeted by DDoS (Distributed Denial of Service), which has resulted in significant damage. Our deep learning models for DDoS attack detection were developed using the most recent CICIDS2017 datasets[15]. These models were then tested against traditional machine learning algorithms. The discovered that the offered models had the maximum accuracy rate of 76.16 percent, which was the best we could find. In our research has discovered that, except for MLP, the accuracy of the other three deep learning methods is greater than 75%, and is even better than that of the machine learning algorithms, which are themselves even better[16].

De La Torre Parra *et al.*(2020) acknowledged that Maker proposes a scattered cloud-based critical learning structure for phishing and Botnet attack recognition and assistance. Two critical security components, in particular, are included in the model and perform as intended: The circulated CNN model is introduced into an ML motor in the customer's IoT device, allowing us to distinguish and protect the IoT device from phishing attacks at the beginning. A CNN model was used to distinguish URL-based attacks coordinated with a customer's IoT devices, which was presented in this research as an IoT tiny security add-on[18].

Latif *et al.*(2020) acknowledged that Artificial intelligence (AI) can be used to predict various network security attacks, including denial-of-service (DoS), vindictive activity, and pernicious control. To counteract these attacks, an original lightweight arbitrary neural organization (RaNN)-based system has been developed based forecast model has been proposed in this article. To examine the presentation of the RaNN-based expectation model, a few assessment boundaries like exactness, accuracy, review, and F1 score were determined and contrasted and the conventional counterfeit neural organization (ANN), support vector machine (SVM), and choice tree (DT)[20].

Waheed et al. (2021) recognized that has been acknowledged that cyber risks are developing at an exponential rate, rendering the present security and privacy solutions ineffective. As a result, everyone on the Internet is a potential source of revenue for hackers. The outcome of this is that Machine Learning (ML) methods are being used on huge complicated datasets to provide trustworthy outputs. The outputs created may then be used to foresee and discover vulnerabilities on Internet of Things-based systems. Several researches has been undertaken on either machine learning algorithms or Bayesian computation. Machine learning algorithms and behavioral analytics techniques can be used to solve both security and privacy problems, but these studies only look at one or the other. This shows that a combined survey of recent efforts to solve both security and privacy problems with machine learning algorithms and behavioral analytics techniques is needed in one place [22]. When it comes to cybersecurity and privacy in the Internet of Things, research has been going on for the last few years, from 2008 to 2019. In this article, we look at some of the research that has been done over that time. The research efforts are broken down into three groups. Security and privacy are important issues for people who use the Internet of Things [23].

3. Methodology

In this part, describe the dataset, tools AI calculations that utilized, and current execution stages. The section gives a short explanation of the dataset utilized and proposed a way to deal with
recognize attacks in IoT Systems. Classification studies are conducted using Python language, a suite of learning machines used for scientific research in data Machine Learning. Unsupervised machine learning techniques are used to discover abnormalities in our suggested strategy. The experimental outcomes show that the classification performance of the proposed solution to measure the cyber security threats in IoT is better than the state of art methods [24].

3.1 Dataset

Machine learning methods for network security require large datasets to distinguish normal from malicious traffic. Over the years, datasets like DARPA 98, KDD99, UNSW-NB15, CICIDS2017, and N-BaIoT have been developed, though many remain private due to security concerns. However, most existing datasets either lack IoT-generated traffic or realistic attack scenarios. To address this, Mustafa et al. created the KDD Cup 99-IoT dataset, containing real and simulated IoT traffic with multiple attack types, including DoS, Probe, U2R, and R2L. Our research used this dataset, available on Kaggle, to test classifiers such as KNN, Logistic Regression, and K-Means Clustering, selected for their popularity and diverse features [11].

3.2 Proposed Methodology

This section gives a quick overview of the dataset we used and how we think we can detect attacks in IoT networks. Machine learning techniques are used to detect anomalies in our proposed approach, which includes a variety of pre-processing steps as well as actual applications.

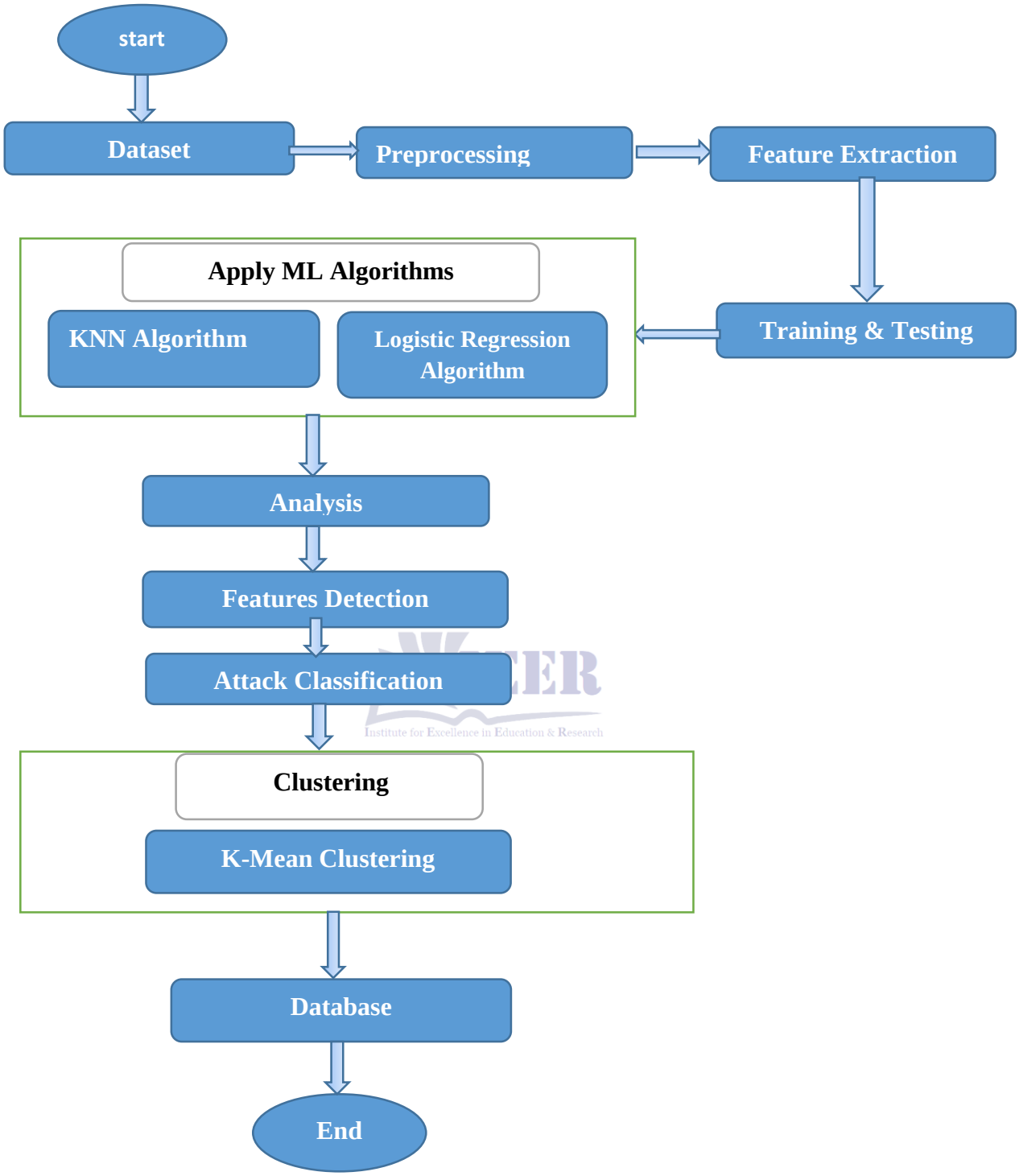

Figure 3: Process Model for IoT Cyber Attack Detection Using ML Algorithms

3.2.1 Feature Extraction
Feature extraction identifies key characteristics from data to better distinguish malicious from benign files, improving classifier prediction accuracy (Ullah et al., 2019).

3.2.2 Data Pre-processing
Involves cleaning and transforming the dataset by removing unnecessary or corrupted data, making it suitable and efficient for machine learning.

3.2.3 Training and Testing
In our research, **80%** of the KDD Cup 99 dataset was used for training and **20%** for testing to evaluate algorithm performance.

3.2.4 Machine Learning Algorithms
The KDD 99 dataset was tested with **K-Nearest Neighbours**, **Logistic Regression (LR) anomaly detection**, and **K-Means Clustering**—chosen for their popularity and diverse features in IoT attack detection.

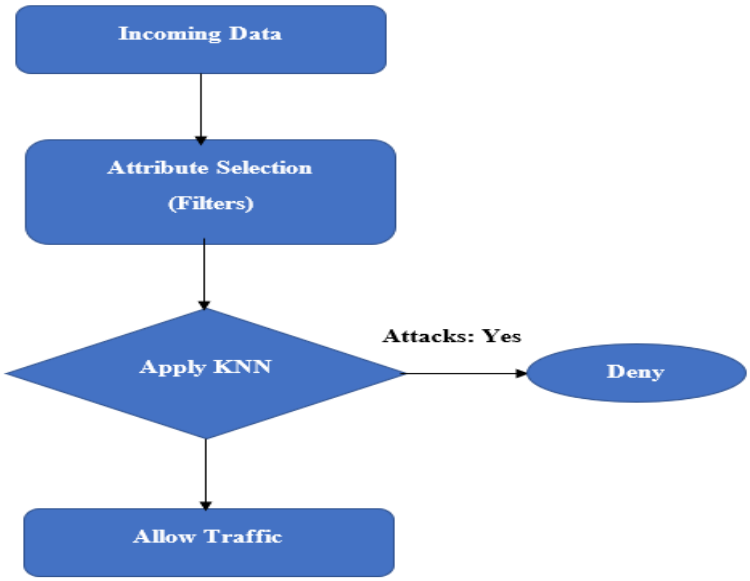

Figure 4: Attack Framework

(i) K-Nearest Neighbors (KNN)
A simple supervised learning algorithm used for classification and regression. It classifies new data points based on similarity to stored examples. KNN performs well across various data types but can be slower in prediction compared to other algorithms.

(ii) Logistic Regression (LR)
A supervised learning algorithm for classification, predicting categorical outcomes (e.g., Yes/No) using probabilities between 0 and 1. Similar to Linear Regression but used for classification instead of regression problems.

(iii) K-Means Clustering
An unsupervised learning method that partitions data into *k* clusters based on similarity. Each cluster has a centroid, and the process repeats until optimal grouping is achieved.

3.3 Analysis
Results are analyzed and compared using static analysis (examining malware without execution) and dynamic analysis (executing malware in a controlled environment).

3.4 Feature Detection
Signature-based detection compares activity patterns to known attack signatures stored in IDS databases. If a match is found, an alert is triggered. Heuristic scanning complements this by detecting suspicious patterns even without exact signature matches.

3.4.1 Detection Methods

The suggested detecting module is shown in Figure 3.7 below. Every one of the recommended techniques will be subjected to the same module procedure. The results will be analyzed later, and the algorithm with the highest performance and accuracy will be selected based on the metrics described before, which are as follows:

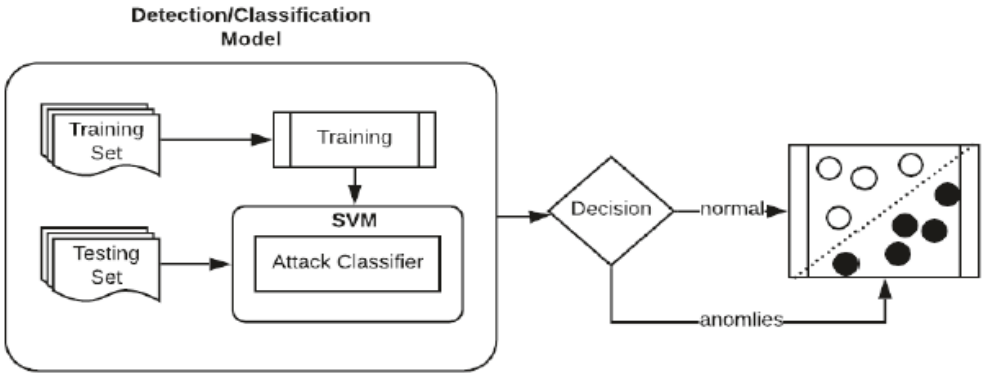

Figure 5: Detection Method

3.5 Classification of Attacks

In this Phase There are four different types of assaults. DoS, Probe, R2L, and U2R are the four types of assaults. The process of assigning a piece of malware to a group of malwares is called malware classification. Malware that comes from the same family has traits that can be used to make signatures for detection and categorization. Based on how they are found, signatures can be either static or dynamic.

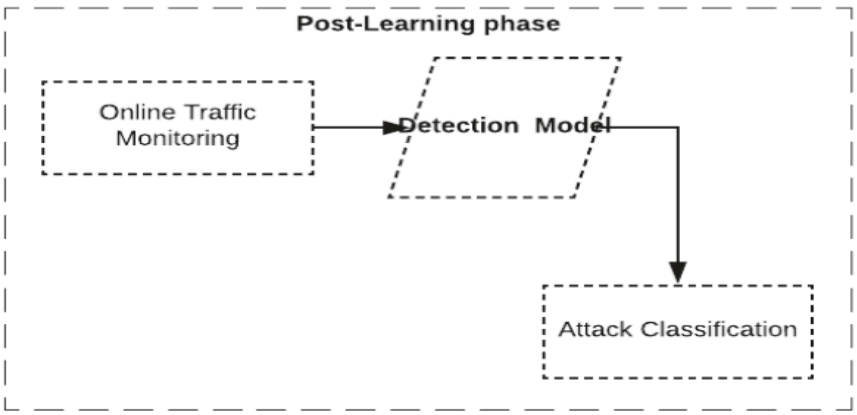

Figure 6: Post learning Phase

A machine learning algorithm When the best method for defending against DoS attacks in IoT has been found, it is chosen and used in the proposed IoT network. This is because it has been found to be the best method for preventing DoS attacks with the fewest false positives and false negatives.

4. RESULTS AND DISCUSSIONS

This chapter describes the results after performing experiment on KDD 99 dataset. The data set consist of various features to identify whether a traffic is a type of attack or normal. The target class consist of

different types of attacks smurf, neptune, back, Satan, ipsweep, portsweep, warez client, teardrop, pod, nmap, guess_passwd, buffer overflow, land, warezmaster, imap, rootkit, load module, ftp writes, multihop, phf, perl, spy. All those attacks are fall into the main categories of the preliminary purpose of this research is to detected different types of attacks on Iot network. We were used KNN and Logistic regression and K-Mean Clustering Machine Learning Algorithm. The proposed approach is found good enough to meet objectives of this research.

4.1 Classification of Attacks

All attack categories contain some specific attack types. In our research the Attacks Categories four Parts like DoS, Probe, U2L, U2R.The Normal attacks is 87832 Dos attack 54572 probe attack 2130 R2L 999 and U2R 52 is given below table. Examples include denial of service (DoS) attacks with six particular attack types (e.g., back, land, neptune), and R2L attacks with eight unique attack types (e.g., ftp write, guess password, imp).

```
normal     87832
dos        54572
probe       2130
r2l          999
u2r           52
```

Figure 7: Classifications of Attacks

4.2 Accuracy of each Attack

Accuracy of each attacks given below. The classifications of each attack describe above that attacks calculate the accuracy in this diagram


```
normal     0.603290
dos        0.374867
probe      0.014631
r2l        0.006869
u2r        0.000343
Name: target, dtype: float64
```

```
ids['target'].value_counts() / len(ids)
```

```
normal     0.603304
dos        0.374846
probe      0.014631
r2l        0.006862
u2r        0.000357
```

Figure 8: Accuracy of Attacks

4.3 Attacks Plotting

In this diagram show the plotting of the above four attacks. The Normal attacks line up after that highest ratio of DoS and probe R2L and U2R as fellow

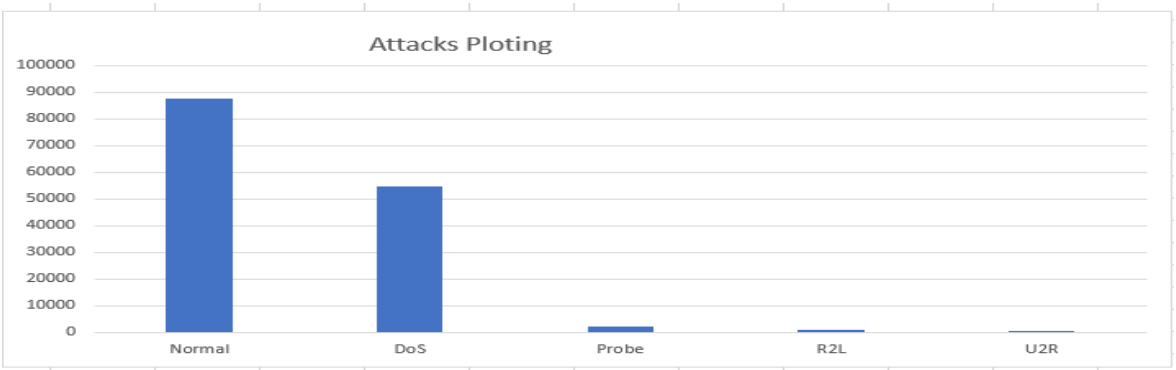

Figure 9: Attacks Plotting

4.4 Protocol Type Vs Target Status

In this diagram show the Protocol type in which attacks are targeted this protocol are tcp, icmp and udp in the diagram. The results show that normal attacks represent blue color and Dos attacks represent orange color and probe attack Green R2L red and U2R purple color.

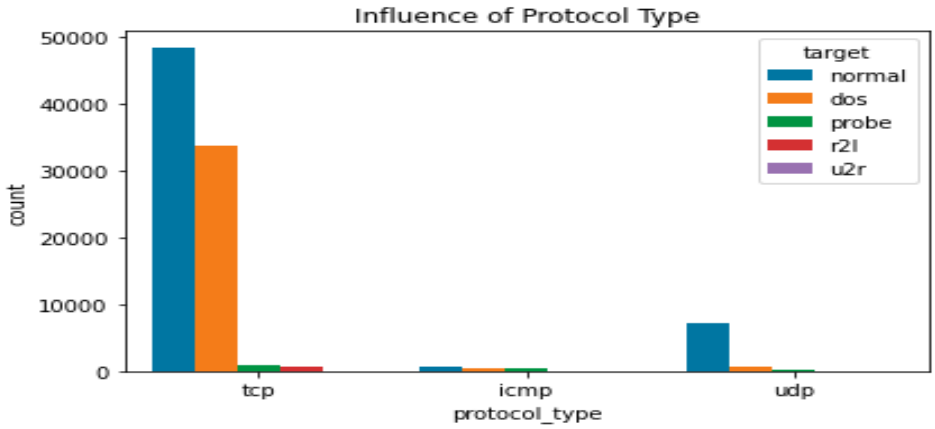

Figure 10: Targeted Protocol Types

Table: 4.1 RESULTS OF THE ALGORITHMS

ML Algorithm	Accuracy	Precision	Recall	F-Measure
Logistic Regression	0.98 %	0.9840	0.932	0.969
KNN	0.97 %	0.9712	0.9728	0.9695

Table: 4.2: CONFUSION MATRIX OF ALGORITHMS

TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Class
0.378	0.386	0.392	0.378	0.385	-0.008	0.496	0.395	DoS
0.000	0.002	0.000	0.000	0.000	-0.002	0.501	0.002	U2R
0.041	0.043	0.043	0.041	0.042	-0.002	0.498	0.045	R2L
0.165	0.174	0.153	0.165	0.159	-0.009	0.496	0.159	Prob
0.402	0.397	0.399	0.402	0.400	0.005	0.503	0.398	Normal
0.338	0.340	0.340	0.338	0.339	-0.003	0.499	0.342	

Following Logistic Regression in Table 1 is the KNN algorithm, which is the best at finding things quickly. Logistic regression is a lot faster than KNN, as a result, it prioritizes this characteristic first from the perspective of the F-measure, there was no significant difference in the performance of the algorithms. However, in terms of performance, all of the algorithms had considerably lower running times than the previous versions.

Table:4.3: COMPARISON OF PERFORMANCE OF THE PREVIOUS ALGORITHMS

Attacks Names	Previous Work		Our Work	
	NB	QDA	LR	KNN
DoS	0.72 %	0.85 %	0.98 %	0.97%
Probe	0.73 %	0.83 %	0.97 %	0.96 %
U2R	0.71 %	0.81 %	0.93 %	0.94 %
R2L	0.70 %	0.80 %	0.94 %	0.91 %

4.15 Comparative Analysis

There is a study in the literature that compares the results of this project to the results of this project (see Table 2). It was chosen for this comparison because it was done by Ferrag et al for their study in 2019. We used two different machine learning methods to do this, but we also used the same dataset and two different methods in the work that was talked about [28]. These algorithms are Nave Bayes and QDA. The detection rate (also known as recall) was selected as the primary criteria for assessment. The outcomes of the two investigations are shown in Table 4.3, which compares them. When the findings are analysed, it becomes clear that the KNN algorithm and Logistic Regression technique utilised in our research are superior than those previously used. As a result, we can observe that our efforts improved the performance of both methods.

4.16 Accuracy, Precision, Recall and F-Measures Graphs

Precision measures how many of these predictions are correct. A positive class prediction was produced for every positive case in the dataset, and this statistic indicates how many positive class predictions were made overall. One way to measure how good a model does on a dataset is to use the F-score, or F1-score. This is how well the model does on the dataset. There is a table below that shows how well each test did in terms of accuracy, precision, recall, and F-Measures.

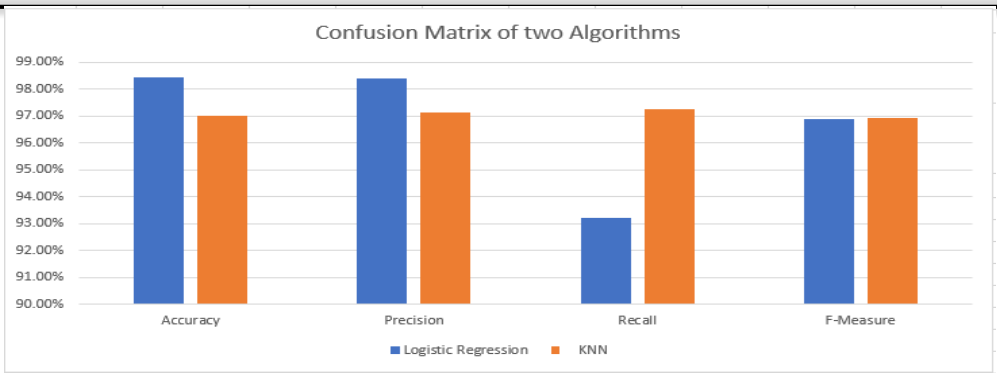

Figure 11: Graph Confusion Metrics

4.19 Graphical Representation of Two Algorithm

The given below graph show the combine results of our both algorithms Logistic Regression and KNN. In this graph show that highest accuracy of in both algorithm in DoS attack after that probe attack 2nd highest accuracy in both graph and 3rd and 4th minor difference in U2R and R2L result in Adaptive algorithm. Both algorithms show the best results in previous algorithms used that dataset

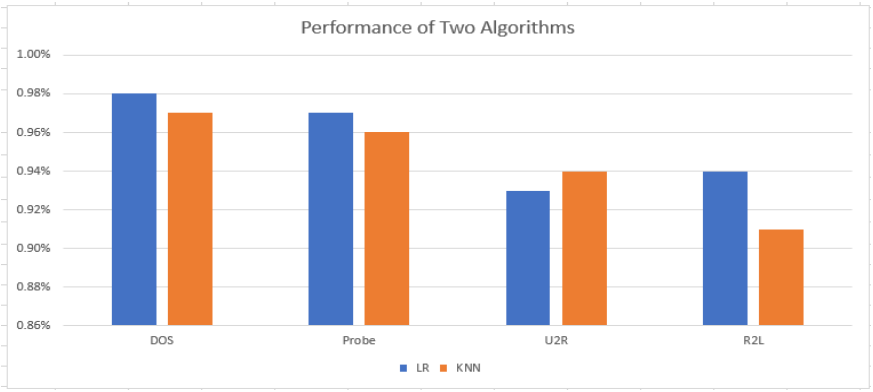

Figure 12: Performance of Two Algorithm

4.20 Graphical Representation of Comparative study

Comparative study shows how two study are similar or shows how two study are different. Most authors are more conservative in their estimate of how long comparative study has been with us. The given below chart show the comparative study of the research. This chart shows the combine results of previous and our research. This chart clearly shows that our research best results then previous. The adaptive boosting algorithm show the best result and accuracy point 0.98% and KNN 0.97%.

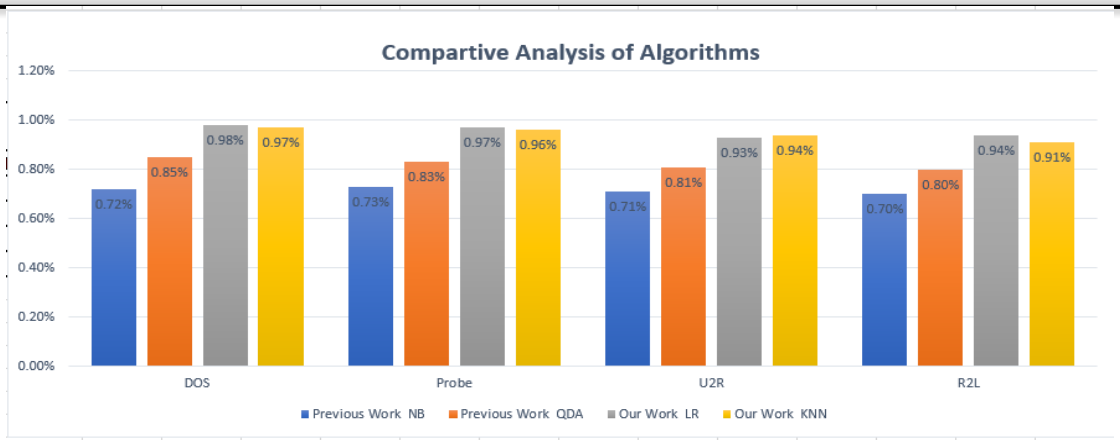

Figure 13: Comparison

Conclusion

The Internet of Things (IoT) has emerged as a transformative technology; however, its rapid growth has introduced significant security challenges. Due to limited resources, insecure designs, and lack of manual controls, IoT devices remain highly vulnerable to cyberattacks such as malware, denial of service (DoS), probing, and unauthorized access. This study demonstrated that Machine Learning (ML) techniques provide an effective solution to strengthen IoT network security by enabling intelligent and automated attack detection. Using the KDD 99 Bot Dataset, multiple algorithms including K-Nearest Neighbor (KNN), Logistic Regression, and K-Means clustering were applied. The results revealed that Logistic Regression achieved the highest accuracy (0.98), slightly outperforming KNN (0.97). These findings indicate that ML-based approaches can significantly improve intrusion detection in IoT networks compared to traditional methods[25,26].

Future research will focus on applying the proposed machine learning techniques to more diverse and larger datasets in order to enhance the robustness, generalizability, and scalability of the approach. Advanced analysis will be conducted for the classification of sophisticated and evolving malicious software targeting IoT environments. Moreover, hybrid models that integrate supervised and unsupervised ML techniques will be explored to further improve detection accuracy, minimize false alarms, and adapt to the dynamic threat landscape of IoT systems [27].

REFERENCES

[1] H. Naeem, "Detection of Malicious Activities in Internet of Things Environment Based on Binary Visualization and Machine Intelligence," *Wirel. Pers. Commun.*, vol. 108, no. 4, pp. 2609–2629, 2019, doi: 10.1007/s11277-019-06540-6.

[2] D. W. Fernando, N. Komninos, and T. Chen, "A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques," *Internet of Things*, vol. 1, no. 2, pp. 551–604, 2020, doi: 10.3390/iot1020030.

[3] K. D. T. Nguyen, T. M. Tuan, S. H. Le, A. P. Viet, M. Ogawa, and N. Le Minh, "Comparison of Three Deep Learning-based Approaches for IoT Malware Detection," *Proc. 2018 10th Int. Conf. Knowl. Syst. Eng. KSE 2018*, pp. 382–387, 2018, doi: 10.1109/KSE.2018.8573374.

[4] A. Ullah, N. Javaid, A. S. Yahaya, T. Sultana, F. A. Al-Zahrani, and F. Zaman, "A Hybrid Deep Neural Network for Electricity Theft Detection Using Intelligent Antenna-Based Smart Meters," *Wirel. Commun. Mob. Comput.*, vol. 2021, pp. 1–19, 2021, doi: 10.1155/2021/9933111.

[5] C. R. Srinivasan, B. Rajesh, P. Saikalyan, K. Premsagar, and E. S. Yadav, "A review on the different types of internet of things (IoT)," *J. Adv. Res. Dyn. Control Syst.*, vol. 11, no. 1, pp. 154–158, 2019.

[6] A. Makkar, S. Garg, N. Kumar, M. S. Hossain, A. Ghoneim, and M. Alrashoud, "An Efficient Spam Detection Technique for IoT Devices Using Machine Learning," *IEEE Trans. Ind.*

Informatics, vol. 17, no. 2, pp. 903–912, 2021, doi: 10.1109/TII.2020.2968927.

[7] M. Talha, T. Bajwa, A. Rasool, M. R. Amin, and M. Jehanzeb, "Multimodal Robustness in Generative AI : Defending Cross-Domain Synthesis," vol. 03, no. 03, pp. 66–82, 2025.

[8] T. Sciences, "ANALYSIS OF THE IoT IMPACT ON VOLUME OF DDoS ATTACKS," *XXXIII Simp. o novim Tehnol. u poštanskom i Telekomun. saobraćaju – PosTel 2015*, pp. 1–10, 2015.

[9] S. Suganth and D. Usha, "a Survey of Intrusion Detection System in Iot Devices.," *Int. J. Adv. Res.*, vol. 6, no. 6, pp. 23–30, 2018, doi: 10.21474/ijar01/7183.

[10] M. Talha, T. Bajwa, and A. Latif, "Resilient Cloud Architectures for Optimized Big Data Storage and Real-Time Processing Article Info," | *Int. J. Adv. Comput. Emerg. Technol.*, vol. 02, no. 02, pp. 1–02, 2025.

[11] I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Comput. Networks*, vol. 188, no. October 2020, p. 107840, 2021, doi: 10.1016/j.comnet.2021.107840.

[12] M. Kalash, M. Rochan, N. Mohammed, N. D. B. Bruce, Y. Wang, and F. Iqbal, "Malware Classification with Deep Convolutional Neural Networks," *2018 9th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2018 - Proc.*, vol. 2018-Janua, pp. 1–5, 2018, doi: 10.1109/NTMS.2018.8328749.

[13] H. Latif, "Predicting Early Heart Disease : A Supervised Machine," vol. 2, no. 3, pp. 229–241, 2024.

[14] M. Roopak, G. Yun Tian, and J. Chambers, "Deep learning models for cyber security in IoT networks," *2019 IEEE 9th Annu. Comput. Commun. Work. Conf. CCWC 2019*, pp. 452–457, 2019, doi: 10.1109/CCWC.2019.8666588.

[15] N. Razzaq, F. Abbas, S. Mehboob, and F. Raoof, "TOMATO LEAF DISEASE DETECTION USING YOLOV9 AND COMPUTER," vol. 3138, pp. 626–638, 2025.

[16] M. Talha, T. Bajwa, A. Rasool, A. Khalid, and M. Jehanzeb, "The Quantum Barrier : Cryptographic Safeguards for Blockchain Integrity," vol. 03, no. 03, pp. 35–48, 2025.

[17] G. De La Torre Parra, P. Rad, K. K. R. Choo, and N. Beebe, "Detecting Internet of Things attacks using distributed deep learning," *J. Netw. Comput. Appl.*, vol. 163, no. April, pp. 1–13, 2020, doi: 10.1016/j.jnca.2020.102662.

[18] U. Tayyab, F. B. Khan, M. H. Durad, and A. Khan, "A Survey of the Recent Trends in Deep Learning Based Malware Detection," pp. 800–829, 2022.

[19] S. Latif, Z. Zou, Z. Idrees, and J. Ahmad, "A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network," *IEEE Access*, vol. 8, pp. 89337–89350, 2020, doi: 10.1109/ACCESS.2020.2994079.

[20] M. K. Alzaylaee, S. Y. Yerima, and S. Sezer, "DL-Droid: Deep learning based android malware detection using real devices," *Comput. Secur.*, vol. 89, 2020, doi: 10.1016/j.cose.2019.101663.

[21] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures," *ACM Comput. Surv.*, vol. 53, no. 6, pp. 1–37, 2021, doi: 10.1145/3417987.

[22] M. A. Gill, M. Ahmad, S. Aziz, M. T. T. Bajwa, and A. Rasool, "Evolution of Cybersecurity in Fintech, A Scoping Review of Literature," *J. Comput. Biomed. Informatics*, vol. 5, no. 01, pp. 326–335, 2023.

[23] N. S. Selamat and F. H. M. Ali, "Comparison of malware detection techniques using machine learning algorithm," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 16, no. 1, pp. 435–440, 2019, doi: 10.11591/ijeecs.v16.i1.pp435-440.

[24] M. Anwer, S. M. Khan, M. U. Farooq, and W. Waseemullah, "Attack Detection in IoT using Machine Learning," *Eng. Technol. Appl. Sci. Res.*, vol. 11, no. 3, pp. 7273–7278, 2021, doi: 10.48084/etasr.4202.

[25] F. Khan, C. Ncube, L. K. Ramasamy, S. Kadry, and Y. Nam, "A Digital DNA Sequencing Engine for Ransomware Detection Using Machine Learning," *IEEE Access*, vol. 8, pp.

119710–119719, 2020, doi: 10.1109/ACCESS.2020.3003785.

[26] Asif, D. M., & Shaheen, A. (2022). Creating a High-Performance Workplace by the determination of Importance of Job Satisfaction, Employee Engagement, and Leadership. Journal of Business Insight and Innovation, 1(2), 9–15.

[27] Asif, M., Pasha, M. A., & Shahid, A. (2025). Energy scarcity and economic stagnation in Pakistan. Bahria University Journal Of Management & Technology, 8(1), 141-157.

[28] Asif, M., Shah, H., & Asim, H. A. H. (2025). Cybersecurity and audit resilience in digital finance: Global insights and the Pakistani context. Journal of Asian Development Studies, 14(3), 560-573.