Advanced Research and Development Journal
ISSN: Applied | Volume 1 Issue 1 | October-December 2025 | Inaugural Edition | ARD-003
www.ardjournal.com | DOI:

AN INTELLIGENT AND SECURE SPAM CLASSIFICATION FRAMEWORK BASED ON SUPERVISED LEARNING

Dr. BURLA SRINIVAS, *Associate Professor,*
Department of CSE,
CMR INSTITUTE OF TECHNOLOGY(AUTONOMOUS), Hyderabad.

ABSTRACT: Numerous sensors and actuators are interconnected via cable or wireless routes to facilitate data transmission. It has experienced significant expansion over the past decade, and by 2020, it is anticipated to be linked to over 25 billion devices. In the forthcoming five years, these devices will convey substantially larger quantities of data than they presently do. The device generates a significant amount of data in many forms, with quality affected by factors including the production source, processing time, and data quantity. Machine learning approaches are crucial for ensuring security and access control in biotechnology, while simultaneously improving safety and efficacy by detecting anomalous behaviors. In contrast, malevolent individuals frequently utilize learning methodologies to exploit system flaws. After evaluating these challenges, we recommend employing machine learning approaches to detect and mitigate spam, thus improving device security. The most effective approach for detecting waste is to utilize an autonomous learning system. This methodology assesses the efficacy of four machine learning models by employing various feature sets and metrics as inputs. All models employ the updated input attributes to ascertain a spam score. This rating, shaped by various elements, indicates the equipment's reliability. The findings demonstrate that the proposed technique is effective in comparison to other well-established systems.

Keywords: Collection of data, Authorization, Anomalous detection, Support Vector Machine, K-nearest neighbour, Spam.

I. INTRODUCTION

Information technology has made it feasible for information to flow directly and quickly. Regardless of where they are physically located, people can communicate with each other through a variety of online channels. When it comes to the worldwide distribution of information, email is unparalleled in terms of speed, effectiveness, and cost. Even if there are other ways to target emails, spam is the most common and harmful. Since it is a waste of time and effort, people hate receiving spam emails.

Furthermore, if these emails include malicious files that pose as attachments or URLs, the host system's security may be compromised. Spam is the practice of sending an unsolicited or needless message to a large number of people. The message could be sent via email or another electronic communication method. Many people want to make their email system safer. Trojan horses, RATs, and system flaws are among the dangerous programs frequently found in spam emails. Perpetrators frequently use this strategy to trick their victims into using their internet services.

Sending unsolicited emails with malicious files or shortened URLs that take users to phony or dangerous websites is one way they steal sensitive data, such as bank account information or personal information. Users can program automated email filters to look for specific phrases across several email providers. Because personalizing emails is so difficult and customers aren't interested, scammers may focus all of their attention on their accounts, rendering this strategy useless.

Over the past few decades, the Internet of Things, or IoT, has become increasingly significant. Many people think that the Internet of Things, or IoT, is essential to the operation of modern smart cities. Many social media sites depend on the Internet of Things (IoT) to operate. An essay titled "Security and Communication Networks" was included in Hindawi Volume 2022. The item's identifying number is 1862888, and it contains 19 pages. As the Internet of Things grows in popularity, more and more people are becoming concerned about spam. For further details, see the paper at. Scientists have created a variety of methods for spotting and preventing fraud and spam.

Currently, spam detection algorithms are separated into two primary categories: behavioral patterns and syntactic patterns. All of these strategies have drawbacks and limitations. Spam emails have become more prevalent as global communication and the Internet have expanded. Spammers can send their messages from any location with an internet connection while hiding their identity. Even though there are many strategies and technological tools available to lessen spam, its prevalence is still quite high. Emails with links to harmful websites that could steal personal information are among the worst types of spam. Spam emails use a lot of memory and storage space, which affects system performance.

To identify and eradicate the issue of spam emails, every company tests a range of spam-fighting techniques within its own infrastructure. To identify and assess incoming emails for spam, a number of tried-and-true techniques are used, including keyword analysis, mail header inspection, and whitelisting and blacklisting. According to social media specialists, an estimated 40% of these networks' accounts are used for spam dissemination. Spammers utilize popular social networking sites to spread concealed links to commercial or pornographic websites in an effort to sell and market their goods. They also use these links to spread phony accounts to review sites, fan sites, and certain demographics.

There are frequently recurrent themes in emails that are harmful to certain individuals or communities. Pay attention to these crucial aspects if you wish to improve your ability to recognize these letters. AI is capable of distinguishing between spam and authentic emails. This method works well because it uses data from the subjects, bodies, and headers of messages. Once the item has been removed, its features can be used to determine if it is spam or ham. These days, a lot of people use machine learning methods to detect spam.

II. REVIEW OF LITERATURE

Researchers Aaisha Makkar, Sahil (GE) Garg, Neeraj Kumar, M. Shamim Hossain, Ahmed Ghoneim, and Mubarak Alrashoud came up with a practical way for Internet of Things devices to identify garbage using machine learning in 2021. This was made possible with the use of machine learning algorithms. A strategy for spam detection using Internet of Things (IoT) devices is presented in this study. The purpose of the machine learning-based method is to detect spam. Machine learning approaches can quickly sort and evaluate spam data, as

mentioned earlier. With enough effort, we can achieve this. In contexts like the Internet of Things (IoT), the authors show how their method substantially enhances the precision and velocity of waste detection. Since there are now answers, it will include an examination of the implementation challenges in its research.

The problem of security for the Internet of Things needs further investigation. Shieh S., Chen C.K., Zhang Z.K., Cho M.C.Y., Wang C.W., Hsu C.W., and K.K. finished the study in 2014. Some of the current security concerns surrounding the Internet of Things (IoT) are explored and examined in this article. Offering a more all-encompassing perspective on the matters brought up, it also draws attention to important areas that necessitate additional investigation. The writers not only take a hard look at the present state of affairs, but also at the specific security needs of IoT devices, such as privacy of data, identification, and network security. They go over some possible ways to strengthen the safety of applications linked to the Internet of Things and ways to do research in this area.

The paper "Blockchain for Internet of Things security and privacy: A case study of a smart home" was written by P. Gauravaram, R. Jurdak, S. S. Kanhere, and Dorri. A group of people worked on the writing. In 2017, it became available to everyone. This essay primarily aims to explore how blockchain technology might enhance the privacy and security of IoT devices. A smart home will be used as an example in the article. Various viewpoints on "smart homes" will constitute the major emphasis of the study. The authors propose a blockchain-based system to guarantee the safe transfer and storage of data by Internet of Things devices. In their 2017 publication "Botnets and Internet of Things Security," E. Bertino and N. Islam investigated the security and privacy concerns related to smart houses. They came to the conclusion that blockchain technology was the sole way to address these problems. In this article, we'll go over the dangers that botnets pose to IoT systems today. The authors look into the likelihood of botnets taking advantage of holes in IoT systems and push for the creation of defenses against it. The results show how important it is to use new security methods to protect IoT devices against cybercriminals and large-scale botnet assaults.

"Communication Security in the Internet of Things: Preventive Measures and Avoiding DDoS Attacks over IoT Network," a 2015 article by C. Zhang and R. Green, expands upon these results. One of the main goals of this research on communication security in networks connected to the Internet of Things (IoT) is to prevent Distributed Denial of Service (DDoS) attacks. The writers describe in detail a security strategy that shields networks and IoT devices from several types of distributed denial of service (DDoS) assaults. This method comprises many steps to guarantee the safety of different networks and devices. In order to guarantee the reliability and security of the Internet of Things, the study's results stress the importance of executing suitable security measures.

A 2011 book titled "The Dark Side of the Internet: Attacks, Costs, and Responses" was released. Kim, W., Kim, C., So, J., and Jeong, O.-R. wrote the book. We will talk about internet hacks, the costs of them, and efforts to lessen their influence in the paragraphs that follow. Phishing, malware, and distributed denial of service (DDoS) were among the cyberattacks studied by the writers. Additionally, the writers analyze the impact of these initiatives on the budget and operations. This report also takes a look at new innovation and ways to stop cyberattacks. The study's framework stresses the need of implementing preventative security measures.

Advanced Research and Development Journal
ISSN: Applied | Volume 1 Issue 1 | October-December 2025 | Inaugural Edition | ARD-003
www.ardjournal.com | DOI:

With the expectation that it will be published and spread, H. Eun, H. Lee, and H. Oh sent the paper "Conditional privacy-preserving security protocol for NFC applications" to a journal in 2013. The major purpose of this essay is to go over a security mechanism that can, in certain cases, protect privacy. With this method, near field communication (NFC) apps can be used. The suggested method allows near-field communication (NFC) devices to connect safely and anonymously while simultaneously protecting user privacy. The authors show that their protocol is applicable to many NFC contexts by incorporating strong security characteristics like mutual identification and data integrity. Their design incorporates these components to do this.

An interesting read is "Neural network-based secure media access control protocol for wireless sensor networks" (R. V. Kulkarni and G. K. Venayagamoorthy, 2009). The primary objective of this research is to present a neural network-based approach to secure media access control (MAC) in WSNs. In order to expedite and safeguard MAC processes, the suggested protocol makes use of neural networks. This ensures the safety of all data sent and received across the network. This system's ability to handle different security threats is proven by the simulation results.

In this piece, we'll go over machine learning and all the ways it may be applied to WSNs, including hacks and approaches. The results were published in 2018 by M. A. Alsheikh, S. Lin, D. Niyato, and H. P. Tan. When it comes to WSNs, machine learning has a great deal of potential uses. The purpose of this research is to examine and prioritize all of these possible uses. In order to fix the most pressing problems with WSNs, the authors go over a number of optimization and machine learning strategies. Data collecting, energy management, and the unearthing of strange artifacts are all examples of such issues. We hope to gain a better understanding of how machine learning has evolved and what it can do to strengthen the safety and efficiency of WSNs from this research.

Articles like "A survey of data mining and machine learning methods for cyber security intrusion detection," released in 2016, provide all the appropriate details. The purpose of this research is to take a look at how data mining and machine learning have come a long way in finding security holes in computers. The inquiry will primarily concentrate on these strategies. There are a number of techniques to identify and avoid potential online dangers. Tasks such as categorizing and finding unusual items fall under this kind of labor. In this paper, the writers analyze the methods used in great detail. Improving intrusion detection systems is the goal of this article, which will weigh the pros and cons of several research directions.

III. PROPOSED SYSTEM

In order to identify spam emails, it is necessary to combine the email's content with machine learning techniques. The TF-IDF method, which emphasizes particular words in the email, can convert the information into numerical features. Afterwards, these traits are used to train machine learning models to provide predictions.

For this project, we will build a system to detect spam emails using the Support Vector Machine (SVM) method. When it comes to binary classification jobs, one popular and effective machine learning technique is the Support Vector Machine (SVM). To train the system, we will use a Kaggle sample that includes both spam and legitimate emails. The most

recent emails will be analyzed using the learned SVM model to evaluate their spam status. This can be accomplished by reviewing the contents of the emails.

The method uses preprocessing processes including stemming, tokenization, and stop word removal to make TF-IDF estimations more accurate and useful. The most important phrases in each email are transformed into a numerical vector using the TF-IDF vectorization technique. Popular machine learning methods that make use of the vectors include Naive Bayes, Random Forest, and Support Vector Machines (SVM). These methods, when applied to labelled training data, produce models that can correctly categorize spam. There are several steps that need to be taken before machine learning can be employed to detect spam in emails. After then, a compilation of all the found emails is made. Every email gets a spam or non-spam label. Tokenization, splitting, and stop word removal are some of the preprocessing processes that are applied to the dataset. A training set and a testing set are then created from the data. The training data teaches a machine learning model—like a Support Vector Machine or a Naive Bayes classifier—to use numerous email attributes. Some of the characteristics include the organization of the email and how often certain terms and phrases are used.

Data Source:

Two potential places to find email data are real-time email sources and the Kaggle dataset. In this section, you will find the source.

Feature extraction:

The Term Frequency-Inverse Document Frequency (TF-IDF) algorithm can be used to transform textual email content into numerical feature vectors.

Model training and evaluation:

Using labeled data, machine learning models like Support Vector Machine, Naive Bayes, and Random Forest can be trained. Evaluate the model's efficacy via measures such as the F1-score, recall, and accuracy.

Real-time spam detection:

Instantaneous spam detection is made easy with the trained model. A paper architectural model shows the interplay and overall operation of the system's numerous parts. This shows how the email spam detection system's many parts work together and are set up to achieve their goals. The graphic depicts the data flow and system architecture, which helps with collaboration and communication on paper.

1. Data Preprocessing:

In order to prepare the email text for feature extraction, this section employs methods such as stemming, stop word removal, and tokenization.

2. Feature Extraction:

This component uses the TF-IDF technique to transform preprocessed text from emails into numerical feature vectors. By giving terms weights based on their frequency of occurrence in emails, the significance of terms for email sorting may be demonstrated.

3. Machine Learning Model:

The machine learning method you choose is detailed here. It could be k-Nearest Neighbors (k-NN), Naive Bayes, Random Forest, or Support Vector Machine (SVM). The annotated

Advanced Research and Development Journal
ISSN: Applied | Volume 1 Issue 1 | October-December 2025 | Inaugural Edition | ARD-003
www.ardjournal.com | DOI:

dataset is used to train the model to differentiate between spam and non-spam emails based on their patterns and attributes.

4. Model Training:

In order to train a machine learning model, this section outlines the process of using email data that has already been cleaned and features removed. The model organizes letters into categories based on their names and other attributes.

5. Model Evaluation:

Memory, accuracy, precision, and F1-score are some of the measures used to assess the trained model's performance in this section. The ability of the model to detect spam emails can be tested more easily with its help.

6. Real-time Email Classification:

Here we see the learned model in action, sorting emails in real time. The system classifies the email as spam if it finds certain traits in it.

7. Output/Results:

Here you may see the results that the system has produced. Classification decisions, statistical data, or images to aid in further research and understanding could all be part of these results.

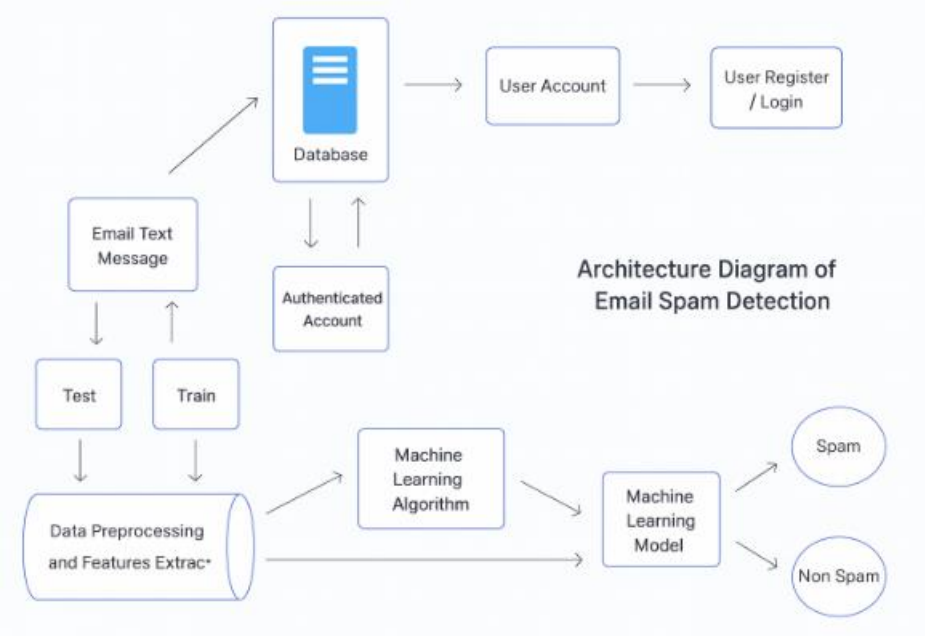

Fig -1: Architecture Diagram of Email Spam Detection

The study's design diagram shows how the parts work together to make the email spam detector more effective. It shows how the data moves through the machine learning process and what each stage does for spam email detection.

IV. RESULTS AND ANALYSIS

The suggested method for detecting email spam has been shown useful and accurate through experiments. This system uses TF-IDF NLP and machine learning to differentiate between spam and real emails. This lessens the possibility of an incident, increases efficiency, and safeguards email. The system's performance is evaluated using standard tests, such as precision, memory, and F1-score. To make sure everything stays there and no one gets overfit, you can utilize methods like stratified sampling and cross-validation.

Advanced Research and Development Journal
ISSN: Applied | Volume 1 Issue 1 | October-December 2025 | Inaugural Edition | ARD-003
www.ardjournal.com | DOI:

Classifiers	Accuracy Score (%)	F1 Score (%)	Precision	Bias-Variance
Support Vector Classifier	98.47%	94.03%	98.52%	0.0596
Naïve Bayes	95.60%	80.32%	1.0	0.1967
Decision Tree	96.41%	85.90%	83.97%	0.1409
K-Nearest Neighbour	93.37%	60.93%	1.0	0.3990
Random Forest	97.04%	87.96%	1.0	0.1203

Table -1: Comparision Table

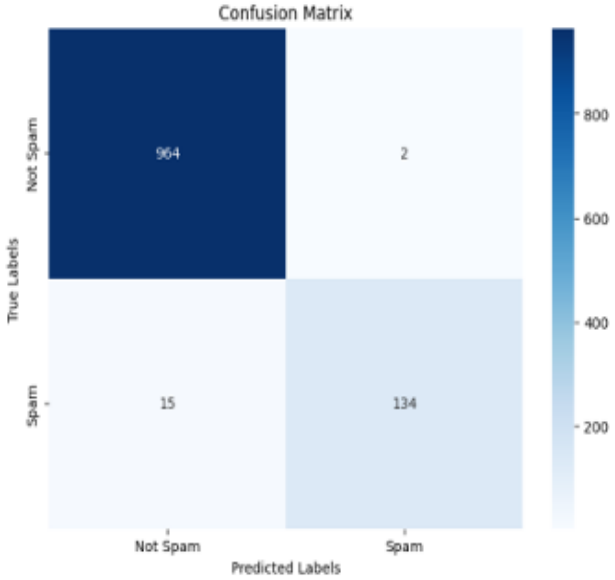

Chart -1: Heatmap Confusion Matrix Chart

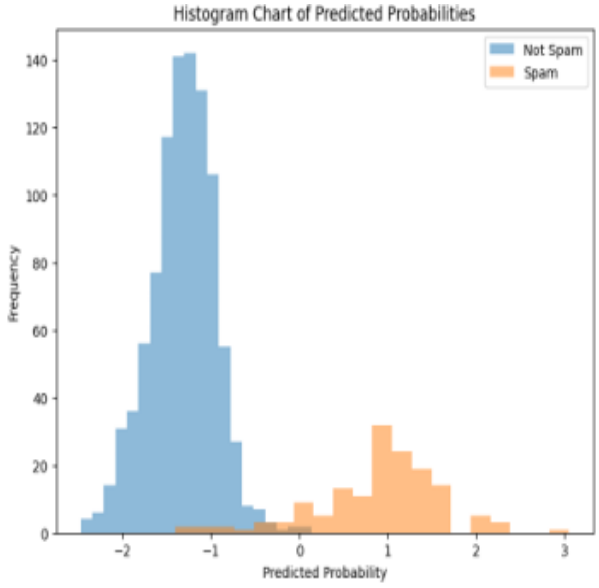

Chart -2: Histogram Chart of Predicted Probabilities Chart

Advanced Research and Development Journal
ISSN: Applied | Volume 1 Issue 1 | October-December 2025 | Inaugural Edition | ARD-003
www.ardjournal.com | DOI:

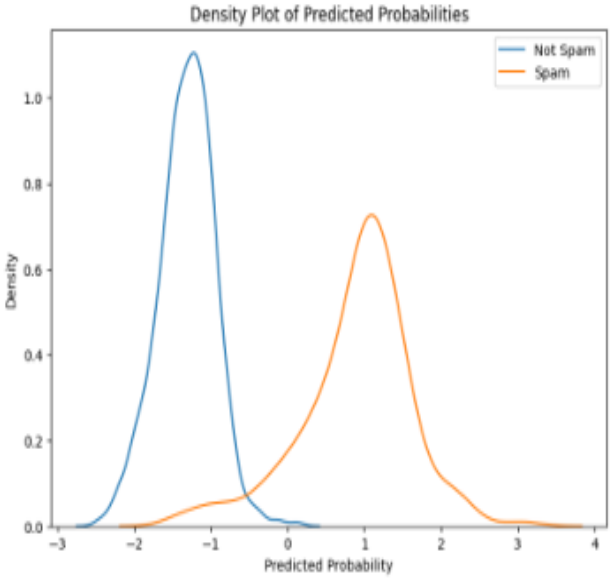

Chart -3: Density Plot Of Predicted Probabilities Chart

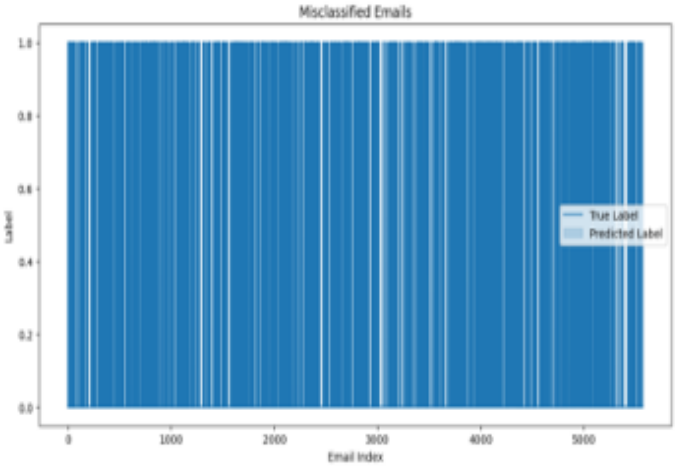

Chart -4: Lineplot Misclassified Emails Chart

Chart -5: Word Cloud Non Spam

Advanced Research and Development Journal
ISSN: Applied | Volume 1 Issue 1 | October-December 2025 | Inaugural Edition | ARD-003
www.ardjournal.com | DOI:

Chart -6: Word Cloud Spam

Classifiers	Mean Error	Values in (%)			
		MSE	MAE	RMSE	R-Square
Support Vector Classifier	1.0	01.52%	01.52%	12.34%	86.83%
Naïve Bayes	1.0	04.39%	04.39%	20.96%	62.04%
Decision Tree	1.0	03.85%	03.85%	19.63%	66.68%
K-Nearest Neighbour	1.0	07.62%	07.62%	27.61%	34.15%
Random Forest	1.0	02.86%	02.86%	16.94%	75.21%

Table -2 : Evaluation Table

V. CONCLUSION

These examples show how the TF-IDF NLP approach, when paired with machine learning, may effectively detect email spam. The suggested solution is a decent approach to deal with the growing problem of email spam since it gives users a simple and secure way to delete annoying messages without risking their security. The goal of this project is to create a reliable method for detecting spam emails so that email security may be enhanced, users can be protected from online dangers, and spam can be less annoying.

REFERENCES

1. Aaisha Makkar, Sahil (GE) Garg, Neeraj Kumar, M. Shamim Hossain, Ahmed Ghoneim, Mubarak Alrashoud,"An Efficient Spam Detection Technique for IoT Devices using Machine Learning" ,IEEE Transactions on Industrial Informatics (Volume: 17, Issue: 2, Feb. 2021)
2. Z. K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, andS. Shieh, "Iot security: ongoing challenges and research opportunities,"in 2014 IEEE 7th international conference on service-oriented computing and applications. IEEE, 2014, pp. 230–234.
3. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smarthome," in 2017 IEEE international conference on

pervasive computing and communications workshops (PerCom workshops). IEEE, 2017, pp. 618–623.
4. E. Bertino and N. Islam, “Botnets and internet of things security,” Computer, no. 2, pp. 76–79, 2017.
5. C. Zhang and R. Green, “Communication security in internet of thing: preventive measure and avoid ddos attack over iot network,” Proceedings of the 18th Symposium on Communications & Networking. Society for Computer Simulation International, 2015, pp. 8–15.
6. W. Kim, O.-R. Jeong, C. Kim, and J. So, “The dark side of the internet: Attacks, costs and responses,” Information systems, vol. 36, no. 3, pp.675–705, 2011.
7. H. Eun, H. Lee, and H. Oh, “Conditional privacy preserving security protocol for nfc applications,” IEEE Transactions on Consumer Electronics, vol. 59, no. 1, pp. 153–160, 2013.
8. R. V. Kulkarni and G. K. Venayagamoorthy, “Neural network based secure media access control protocol for wireless sensor networks,” in 2009 International Joint Conference on Neural Networks. IEEE, 2009, pp. 1680–1687.
9. M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, “Machine learning in wireless sensor networks: Algorithms, strategies, and applications,”IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1996–2018, 2014.
10. L. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection,” IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2