Protecting the Internet of Things (IOT) with Machine Learning and Deep Learning Techniques

[1]Jayashree J
Assistant Professor,
Computer Science Department
Srinivas Institute of Technology, Mangalore

[2]Vishnu P. J
Engineer, iOS Development
CodeCraft Technologies Pvt Ltd, Mangalore
pjvishnu705@gmail.com

Abstract- Deep learning (DL) and Machine learning (ML) as an IoT paradigm have improved problem-solving, and as a result, their application has expanded to many different fields. This has led to the idea that there are two powerful ways to use data—deep learning (DL) and machine learning (ML)—to solve specific problems. Thus, this article's objective is to provide a thorough analysis of "Scanning Machines and Deep Learning Techniques for Internet of Things (IOT) Security and Privacy," which addresses the current state of IoT research as well as its joint endeavor with DL. This technique stops the adversary from discovering the training data for the target model by utilizing differential privacy. The research's authors concluded that machine learning and deep learning algorithms were developed relatively recently and were never intended for use in cryptography applications. However, researchers with the necessary skills can use deep learning and machine learning to develop cryptography.

Index Terms- Internet of Things, Deep Learning, Machine Learning, Security

1. INTRODUCTION

The Internet of Things, or IoT, is a network of networked devices, each with an individual identity and the ability to gather and share data with other devices on the network on its own. IoT devices are utilized by various domains and sectors, such as consumer, business, and government applications. The goal and objective of the billions of devices connected to the internet worldwide are the same. Their increasing prevalence in our daily lives has drawn more attention to the inherent safety concerns they pose.

Due to its ease of computation, the integration of machine learning, deep learning (ML), and deep learning (DL) as an Internet of Things (IoT) model helped solve the problem. As a result, the model has been widely adopted in many domains to be used in problem-solving tasks. This led to the development of the ideas of deep learning (DL) and machine learning (ML) methods for analyzing and assessing data in order to distinguish between "abnormal" and "normal" behavior in components and devices.

Internet of Things components are connected to each other in their environment. Furthermore, because DL/ML techniques are able to effectively detect new impending unknown threats by learning from previous attacks, they can be very helpful in identifying new threats, which are often modifications of existing threats. Versions of current threats are often modified to create new ones. For Internet of Things (IoT) systems to be efficient and safe, they must be able to move from secure device-to-device and intelligence-based communication to machine learning and deep learning technologies. Ray and associates, 2016. The terms "symmetric encryption," "differential privacy," "trusted execution," and "ecology" refer to a number of multifaceted strategies for bridging security and privacy gaps in Data and Machine Learning. These strategies are being employed. The most widely used DL and ML privacy technique is known as secure multiparty computing. This approach uses differentiable privacy. which keeps a rival from discovering the use cases that the target model was built using (Aijaz Ali Khan, 2022). (D.G M., 2019).

Symmetric encryption and secure multiparty processing are used in tandem to protect training and test data from unwanted access. Hardware-dependent security and isolation are used in trusted execution environments to safeguard sensitive data and training code. This contributes to the safety of the code and data. On the one hand, these methods greatly add to the processing load and necessitate the application of a specific technique to each type of neural network.

Privacy concerns in both the DL and ML domains have not been adequately and widely acknowledged addressed. Numerous security techniques have been proposed to offer protection from hostile attacks. These methods can be divided into three groups: malware detection, model resilience augmentation, and input processing. Preprocessing involves operations like image modification, randomization, and noise reduction with the goal of reducing the model's dependency on data. These are the kinds of operations that, for the most part, don't require updating or retraining the model. In order to increase model stiffness through model retraining and modification, the second category comprises techniques like trait reduction, regulation, adversarial training, and other approaches.

The strategies covered in the first group are also included in this group. Three-scale detection methods that can be used before the first model layer include adaptive noise reduction and the detection of image transformations. The discovery of a hidden layer is another example. To the best of our knowledge, no defensive tactic can offer complete defense against hostile circumstances (Dattatray G. Takale, 2022). even though several other defensive strategies have been proposed. To combat hostile circumstances, the most effective strategy currently in use is training against one's adversaries. The two main defenses against chemical attacks are as follows. The first tactic is an odd selection method that removes anomalies from the pertinent collection (Aijaz Ali Khan, 2022).

During the second phase, you will attempt to make the neural network more resistant to contamination from tainted samples.

Furthermore, a wide range of research on the Internet of Things enhancements and applications enabled by DL technology has been published in the pertinent academic literature. However, the vast majority of them focus on a specific aspect of IoT or DL.

Consider a survey regarding the application of big data analytics to the Internet of Things. It is impossible to have privacy without security because the two are mutually exclusive. However, security and privacy can coexist. While the privacy of your personal information is more narrowly focused on only that aspect of your information, confidentiality protects the availability, integrity, and confidentiality of information.

Protecting people's privacy is crucial when processing personally identifiable information, but information security is primarily concerned with preventing unauthorized access to different information sources. Any information that is specific to an individual for example, their name, address, social security number, bank account information, login credentials, and so forth may be deemed personal data. Additional instances consist of. Numerous IoT scenarios and applications raise the possibility of more complex and devastating attacks similar to Mirai.

Protecting people's privacy is crucial when processing personally identifiable information, but information security is primarily concerned with preventing unauthorized access to different information sources. Any information that is specific to an individual for example, their name, address, social security number, bank account information, login credentials, and so forth may be deemed personal data. Additional instances consist of. Numerous IoT scenarios and applications raise the possibility of more complex and devastating attacks similar to Mirai.

This article's goal is to provide a thorough analysis of the most recent research on Internet of Things (IoT) scanners for security and privacy, as well as learning strategie. Learn more about the Internet of Things to help you succeed in DL. (Takale S. S. Takattatray G., 2022)

One significant and important consequence of the widespread application of IoT is that it will directly lead to the deployment of IoT becoming a linked effort. Internet of Things (IoT) systems, for example, have to simultaneously take into consideration energy efficiency, security, big data analytics approaches, and interoperability with software applications during the implementation stage.

While examining advancements in a different field, one component cannot be disregarded [9]. Scholars operating across disciplinary boundaries now have a new avenue to explore when examining the difficulties that the Internet of Things systems are currently facing. This integration makes this possible. The distributed nature of Internet of Things devices, which produces a big surface area that is vulnerable to attack, does, however, present additional security issues with this integration. The fundamental issue, which is the growing surface area, is directly responsible for these challenges [10]. This feature of Internet of Things devices raises a lot of concerns for the privacy and personal safety of users.

Furthermore, a significant amount of data generated by the Internet of Things platform is available for use. There is a significant risk that people's privacy will be violated if these data are not evaluated and provided in a secure environment [7].

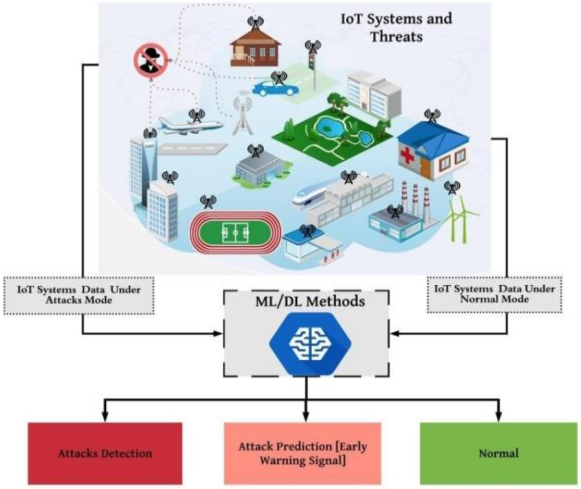
IoT Systems and Threats
IoT Systems Data Under Attacks Mode
ML/DL Methods
IoT Systems Data Under Normal Mode
Attacks Detection
Attack Prediction [Early Warning Signal]
Normal

Fig 1: Illustration of the potential role of ML/DL in IoT security

As demonstrated in Figure 1, the capacity to keep an eye on IoT devices makes it possible to intelligently provide a defense against novel or zero-day attacks. You can use advanced data exploration techniques like machine learning and deep learning (ML/DL) to determine what "normal" and "abnormal" behavior is in terms of how internet of things devices and components interact with one another inside the ecosystem. By gathering and examining data from every IoT device, we can spot behavioral anomalies and stop threats in their tracks.

ML and DL algorithms have the potential to be useful in predicting new attacks, which are frequently variations of previous attempts, because of their ability to intelligently anticipate future unknown assaults by learning from recent events. This is because the majority of contemporary attacks are merely reimagined versions of earlier ones. This means that IoT systems must provide security-based intelligence supported by deep learning and machine learning techniques in addition to enabling secure communication between devices in order to be reliable and safe[10,11].

2. REVIEW OF LITERATURE

Many researchers have studied IoT security in order to provide insight into the current state of the field and its future directions. However, he has recently focused less on applying ML and DL to the field of IoT security in his work. Recent studies have addressed various aspects of Internet of Things systems that may be vulnerable, including encryption, authentication, access control, cyber security, and application security. Kumar et al. (2017) focus on the system's communications security after going over the problems and possible fixes associated with it. Many assessments and studies have been conducted on the Internet of Things (IoT) with the goal of illuminating potential future threats.

Although there has been much discussion on IoT security, no research has been done on the use of DL or ML to guarantee the security of IoT devices. Kumar et al. (2017) felt that regulations and improvements were needed in the following areas: cyber security, application security, encryption, access control, and authentication. Sfar et al. (2018) studied the issues surrounding IoT communication security and possible fixes. Zhao et al. (2013)

conducted comparable research on an intrusion detection system for the Internet of Things.

Furthermore, the IoT framework for regulatory approaches and regulatory concerns may define security and privacy needs (Bengio et al., 2015). An essential component of a distributed IoT infrastructure is privacy and security. The effectiveness of this endeavor was hindered by several factors. Although there are numerous issues that need to be resolved first, researchers believe that the distributed IoT model offers a number of privacy and security benefits.

Numerous conventional ML methods were examined, in addition to state-of-the-art methods that use DL for typical large data sets. The integration of diverse machine learning techniques with signal processing technologies was the main focus for the analysis and investigation of pertinent big data applications. a thorough evaluation of modern DL techniques. The examination covered their current open research problems as well as the background and practical uses of a number of proposed solutions.

The fundamental ideas of several different deep learning models were compared and contrasted, with examples of applications for these models and the progress that has been made in fields such as computer vision, pattern recognition, and voice processing. We surveyed the state of the art in DL for recommendation models for the benefit of mobile advertising. (Takale S. S. Takattatray G., 2022). Furthermore, self-organizing networks employed a range of successful machine learning techniques. Several approaches were analyzed for their advantages and disadvantages, and suggestions for additional research were made. Future network topologies incorporating AI were also considered, along with the associated challenges and opportunities.

Everyone was made aware of how crucial artificial intelligence is in a 5G setting. In [1,2] and [3], data mining was covered in relation to network intrusion detection. Everyone was also made aware of the fact that these applications present unique research challenges of their own. Furthermore, an analysis of a mobile multimedia app that utilized DL was conducted. Some of the topics covered in this discussion included current developments in DL applications (G, 2019), including cutting edge applications in speech recognition and language translation, mobile ambient intelligence and mobile security, mobile healthcare, and mobile wellness.

Everyone was made aware of how crucial artificial intelligence is in a 5G setting. In and [1,2], data mining was covered in relation to network intrusion detection. Everyone was also made aware of the fact that these applications present unique research challenges of their own. Furthermore, an analysis of a mobile multimedia app that utilized DL was conducted. Some of the topics covered in this discussion included current developments in DL applications (G, 2019), including cutting edge applications in speech recognition and language translation, mobile ambient intelligence and mobile security, mobile healthcare, and mobile wellness.

The occurrence of such a situation showed that even highly evolved mechanisms, like traditional machine-learning algorithms, struggle over time to identify minute variations of attacks. In order to ascertain the overall level of network security, Ramos et al. [3] conducted a survey that concentrated on model-based quantitative security measures. A thorough literature review of the state of the art in network security metrics (NSMs) is published in this study. The research primarily focuses on the Common Vulnerability Scoring System (CVSS) framework because it is a foundational element of numerous other security metric models. Studies have also looked into the gaps between security metrics and related fields.

This paper offers a comprehensive and in-depth review of the primary measure proposals, with a focus on the field of model-based quantitative NSMs. An in-depth analysis of the main measure concepts has been included as an extra benefit. Included are all of the main advantages and disadvantages of the studied works. A comprehensive analysis of the salient features of the security metrics under examination was provided at the conclusion, along with a list of outstanding problems and prospective research subjects. A discussion of earlier research in the same field was then held. Given the data presented here, one could argue that much more work is necessary to advance the field of model-based quantitative NSMs, which is still in its infancy.

Granjal et al. [1] pointed out that similar security measures would be advantageous for users of other Internet infrastructures, such a cloud computing and the Internet of Things (IoT), whose security has drawn more attention recently.The Al-Fuqaha group [2]. Investigated were difficulties and problems with IoT deployment strategy and execution, as well as IoT's connections to big data analytics, cloud computing, and fog computing. An innovative intelligent approach to data aggregation, protocol adaptation, and autonomous management is presented in this study. The goal of this endeavor was to improve horizontal integration between IoT services. They discussed the various types of protocols and patterns that can be found in various IoT ecosystem components, looked at IoT standards and protocols, and discussed how they operate.

Investigated were difficulties and problems with IoT deployment strategy and execution, as well as IoT's connections to big data analytics, cloud computing, and fog computing. An innovative intelligent approach to data aggregation, protocol adaptation, and autonomous management is presented in this study. The goal of this endeavor was to improve horizontal integration between IoT services. They discussed the various types of protocols and patterns that can be found in various IoT ecosystem components, looked at IoT standards and protocols, and discussed how they operate. A novel method of network intrusion detection that was especially created for an Internet of Things network was introduced by Lopez-Martin et al. [3].

The proposed method uses a specific type of Conditional Variational Auto encoder (CVAE) that embeds the intrusion labels into the decoder layers. This makes it possible to use the method. The provided model can be used not only for feature reconstruction but also as a component of network monitoring systems, specifically in Internet of Things networks, by integrating it with the current Network Intrusion Detection System.

The recommended approach only needs one training phase, which significantly reduces the amount of computing resources needed. Fu et al. [3] proposed that the Internet of Things would eventually be a part of 5G networks. However, because IoT devices have limited resources, many security techniques are difficult to implement because IoT safety is inevitably linked to many important future 5G scenarios. With regard to the vast and varied IoT networks, a strategy based on automata has been proposed in this work. By comparing the action flows of the various components, the technique uses an extension of Labelled Transition Systems to provide a standard definition of Internet of Things (IoT) systems that can detect intrusions.

3. A REVIEW OF THE APPLICATIONS OF DEEP LEARNING AND MACHINE LEARNING IN IOT SECURITY

The unique approach that learning algorithms take to problem solving has led to their broad adoption in numerous real-world applications. These kinds of algorithms take care of the construction of machines that automatically learn better through use. Learning algorithms have been applied in many different contexts in recent years. The recent advances in the field of learning algorithms have been fueled by the development of new algorithms, the availability of vast amounts of data, and the introduction of algorithms with low processing costs. Machine learning and deep learning have advanced significantly in recent years from their beginnings as scientific curiosity to functional equipment with a broad range of significant applications [11].Conversely, deep learning techniques, or DL methods, are new developments in learning that use multiple non-linear processing layers for generative or discriminative feature extraction. The main method used by DT-based algorithms to classify data is to arrange samples according to the feature values that they have. The branches of a tree, also called edges, each suggest a value that a vertex in a sample that is being classified may have, and the tree's vertices, also called nodes, each represent a feature.

The samples are grouped based on the feature values they possess, with the origin vertex serving as the starting point. The characteristic that most successfully divides the training samples is found to be the tree's origin vertex [10]. Two of the variables that are used to find the optimal feature that best divides the training samples are the information gain [11] and the Gini index [12].

The Bayes theorem [8], which takes into account past knowledge about that event, explains the probability of an event. You can use this page to search for Bayes' theorem. For example, DDoS attacks are detected using network traffic data. Using historical traffic data, the Bayes theorem is one method for estimating the probability that network traffic will be connected to an attack or not. The Naive Bayes (NB) classifier [5], a popular machine learning technique, is predicated on Bayes' theorem.

One popular supervised classifier that is well-known for its ease of use is the NB classifier. Under the presumption of feature independence, NB computes posterior probability and applies Bayes' theorem to predict the likelihood that a given feature set of unlabeled examples fits a given label[6].

As an illustration, for traffic as either normal or abnormal using intrusion detection, NB. Even though these features may depend on one another, the NB classifier treats the features that can be used for traffic classification—such as connection duration, connection protocol (such as TCP and UDP), and connection status flag independently. The modifier "naïve" is used in NB classification because each feature individually influences the likelihood that the traffic is normal or abnormal.

The primary benefits of NB classifiers are their robustness to irrelevant features (the features are preserved independently), simplicity, ease of implementation, applicability to binary and multi-class classification, low training sample requirement, and low training sample requirement. NB classifiers, however, are unable to extract meaningful information from the connections and interplay between features (Dattatray G. Takale S. U., 2022). The relationships between features can be crucial for precise classification, especially for complicated tasks where the relationships between features can greatly improve the classifier's ability to discriminate between classes.

One method that doesn't rely on parameters is the KNN approach. KNN classifiers frequently employ the Euclidean distance as their distance metric. Figure 6 illustrates the KNN classification method and how new input samples are categorized. The actions represented by the green circles in the image are thought to be typical of the system, whereas the actions represented by the red circles are thought to be malevolent. The sample that was previously unidentified must be classified as either typical or malevolent behavior, as indicated by the blue circle. In other words, the KNN algorithm determines the category of unknown samples based on the vote that receives the most support from its neighbors.

The KNN classifier uses the votes cast by a subset of its closest neighbors to assign a category to a new example. For instance, in Figure 6, the class of the unseen sample will be classified as normal behavior if the KNN classification is based on the behavior of the one closest neighbor (k = 1) (Dattatray G. Takale R. R., 2022).

The KNN classifier will classify the unseen sample's class as normal behavior if the KNN classification is based on its two nearest neighbors (k = 2). This is because the two circles that are closest to the unseen sample are green, which represents normal behavior. The KNN classifier will classify the unknown sample's class as malevolent conduct if the KNN classification is based on the three and four nearest neighbors (k = 3, k = 4). This is because all four of the circles that are closest to the unknown sample are red, indicating malicious behavior. One crucial step in figuring out what value of k produces the best results for a given dataset is the cross-validation process.

One of the steps in this procedure is testing multiple k-values. Although the KNN method is a straightforward classification technique that works well with large training datasets, the optimal value for k will always depend on the datasets [9, 10]. Finding the ideal value of k could therefore be difficult and time-consuming. The RFs fall under the group of learning algorithms for supervised learning. Several DTs are built and then integrated in order to produce a reliable and accurate prediction model in an RF and improve overall results [12]. As a result, an RF is composed of many trees that are trained to vote for a particular class and are constructed in a random order.

The category with the highest number of votes is the final outcome of categorization. The RF classifier is primarily constructed using DTs, but these two classification techniques are very different from one another. A DT network will normally produce a set of rules when the training set is first introduced. These rules are then used to classify any new inputs that are added to the network. Nevertheless, since RF requires the building of numerous DTs, its implementation may be challenging in some real-time applications in which a large training dataset is required. RF is resistant to over fitting because it uses decision trees (DTs) to generate subsets of rules for voting on a class. As a result, the classification output is the average of the outcomes, and RF is efficient. Additionally, feature selection may be skipped using RF, and it only needs a few input parameters.

This is a result of RF's need to use multiple datasets to train its models. Radio frequency (RF) techniques are used to detect network anomalies and intrusions. In a previous study, RF, SVM, KNN, and ANN were trained to detect DDoS in IoT systems. RF produced marginally better classification results than the other classifiers when smaller feature sets were used to reduce extra computational overhead and increase the system's suitability for real-time classification. (Takale R. R. Takattatray G., 2022).

4. CONCLUSION

The security requirements for internet of things devices are becoming more complex because many technologies, from physical devices and wireless connections to mobile and cloud architectures, need to be protected and integrated with one another. Deep learning and machine learning advances have led to the development of some powerful analytics tools that could be used to improve IoT security. This study looks into a range of threats to the Internet of Things (IoT) and potential attack points for the technology (Dattatray G. Takale S. D., 2022). The application of machine learning (ML) and deep learning (DL) techniques to Internet of Things (IoT) security is covered in detail in this article.

Next, we assess the advantages and disadvantages of different technologies and their potential applications in safeguarding the Internet of Things (IoT).The machine learning and deep learning methods that enable the underlying Internet of Things layers—the knowledge, network, and application layers—are then examined. To put it briefly, a lot of research has been done using a lot of DL models in a range of IoT domains; however, there are still a lot of problems, obstacles, and possible future directions in the application of DL. Make sure to make use of DL. Utilize deep learning and machine learning effectively to safeguard categorized, managed, and secure Internet of Things systems. Instructional strategies include how to create robust detection models, how to use models to ensure security and privacy, and how to create deep learning models that efficiently utilize the generated heterogeneous IoT data.

Last but not least, some security trade-offs in IoT applications; concurrent integration of ML and DL with block chain for Internet of Things security; and machine learning and deep learning for Internet of Things security in an interactive, networked, and interdependent environment of IoT systems. The goal of this study is to provide a useful manual that could inspire researchers to improve Internet of Things (IoT) system security. This enhancement can take the form of creating end-to-end intelligent IoT development or just enabling secure communication between IoT components.

The research report comes to the conclusion that algorithms for machine learning and deep learning are relatively new and are not intended for use in cryptography applications. Nonetheless, researchers with the ability to perform cryptography may use deep learning and machine learning to implement cryptography. In a similar spirit, Alaba (2017) proved that DL algorithms are capable of deciphering cipher frames by demonstrating their capabilities. The machine learning algorithms and logical procedures that were previously employed have largely been replaced by CNN and AE algorithms.

RNNs have demonstrated the ability to learn how to decode the data that is fed to them. Using an LSTM network with 3,000 units, the internal representations of this encoder can be successfully analyzed for the purpose of decoding fuzzy machine data on RNNs. Among other things, the results of the systematic review carried out for this study show that deep learning algorithms like

RNN can find and analyze polyalphabetic ciphers for cryptanalysis. The advancement of deep learning and machine learning research could expedite the Internet of Things' development. Because so many intelligent objects are connected to devices that are a part of the internet of things, it is imperative that the endpoints of these devices be protected.

Conversely, the consistent benefits of IoT DL models are delineated, along with key domains for future IoT DL research development.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: a survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tut. 17 (4) (2015) 2347– 2376 [Online]. Available, doi:10.1109/ comst.2015.2444095.

[2] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, J. Lloret, Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in IoT, Sensors 17 (9) (2017) 1967 [Online]. Available, doi:10.3390/ s17091967. [46] Y. Fu, Z. Yan, J. Cao, O. Koné, X. Cao, An automata based intrusion detection method for internet of things, Mob. Inf. Syst. (2017) 1–13.

[3]M.AbomharaandG.M.Klien,(2015).“Cybersecurityandtheinternetofthings:Vulnerabilities,threats, intrudersandattacks,”JournalofCyberSecurityandMobility,vol.4,no.1,pp.65–88.

[4]DiroA.andN.Chilamkurti,(2018).“LeveragingLSTMnetworksforattackdetectioninfog-to thingscommunications,”IEEECommunicationsMagazine,vol.56,no.9,pp.124–130,2018

[5]Ray,S.Y.Jin,andA.Raychowdhury,(2016)“Changingcomputing paradigmwithinternetofthings:atutorialintroduction,”IEEEDesign&Test,vol.33,no.2,pp.76–96,2016.

[6]Rajkumar,R.I.Lee,L.Sha,andJ.Stankovic,(2010)“Cyber-physicalSystems:TheNext ComputingRevolution,”inProceedingsoftheDesignAutomationConference,pp.731– 736,IEEE,Anaheim,CA,USA,June2010

[7]Bengio,Y.andG.Hinton,(2015).“Deeplearning,”Nature,vol.521, no.7553,p.436.

[8]Sfar,E.A.RNatalizio,Y.Challal,andZ.Chtourou,(2018).“AroadmapforsecuritychallengesintheInternetof Things,”Digit.Commun.Netw.,vol.4,no.2,pp.118–137,Apr.2018.

[9]Sicari,S.A.Rizzardi,L.A.Grieco,andA.CoenPorisini,(2015).“Security,privacyandtrustinInternetofThings:Theroadahead,”Comput.Netw.,vol.76,pp.146–164,Jan.2015.

[10]Alaba,F.A,M.Othman,I.A.T.Hashem,andF.Alotaibi,(2017).“InternetofThingssecurity:Asurvey,”J.Netw

[11]Comput.Appl.,vol.88,pp.10–28,Jun.2017

[12]DG Takale, VN Khan (2023). Machine Learning Techniques for Routing in Wireless Sensor Network, IJRAR (2023), Volume 10, Issue 1.