Securing the Internet of Things (IOT) Using Deep Learning and Machine Learning Approaches

[1]Dr. Dattatray G. Takale, [2]Mr. Gopal B. Deshmukh
[1-2]Assistant Professor
[1-2]Vishwakarma institute of information Technology, Pune

Abstract: *As a result of the improved problem-solving made possible by the introduction of machine and deep learning (ML) (DL) as an IoT paradigm, its use has spread to a wide variety of fields. This has given rise to the belief that deep learning (DL) and machine learning (ML) are two potent approaches to data for the purpose of solving a particular issue. Consequently, the goal of this article is to give a comprehensive analysis of "Scanning Machines and Deep Learning Techniques for Internet of Things (IOT) Security and Privacy," which discusses the present status of research on IoT and its combined venture with DL. With the use of differential privacy, this method prevents the adversary from learning the training data for the target model. The authors of the research came to the conclusion that deep learning and machine learning algorithms were very recently created and were never meant to be used in cryptography applications. Yet, machine learning and deep learning may be utilized to build cryptography by researchers who are capable of doing so.*

Keyword- *Internet of Things, Deep Learning, Security*

1. INTRODUCTION

The Internet of Things (IoT) is a network of interconnected devices, each of which has a unique identity and is capable of autonomously collecting data and exchanging it with other devices on the network. Applications geared at consumers, businesses, and even the government is all examples of domains and sectors that make use of IoT devices. There are billions of gadgets connected to the internet all around the world that have the same goal and objective. Because of their growing use in our day-to-day lives, the inherent safety concerns that they provide have received more attention [15]. The incorporation of machine learning and deep learning (ML) and DL as an Internet of Things (IoT) model assisted in the problem's resolution due to the ease of computation, which led to the widespread adoption of the model in numerous domains for the purpose of applying it in the task of problem-solving. Because of this, the concept of deep learning (DL) and machine learning (ML) techniques for evaluating and examining data in order to differentiate between "abnormal" and "normal" behavior in devices and components emerged as a result. Components of the Internet of Things are linked to one another within their surroundings. Furthermore, DL/ML techniques can be of great importance in identifying new threats, which are frequently modifications of existing threats, because these techniques are able to effectively detect new impending unknown threats by learning from previous attacks. New threats are frequently modified versions of existing threats [16]. Because of this, Internet of Things (IoT) systems need to be able to transition from safe communication between devices and intelligence based on security to machine learning and deep learning technologies in order to be both secure and efficient. (Ray and colleagues, 2016). Symmetric encryption, differential privacy, trusted execution, and ecology are the names of several multidimensional approaches to resolving the boundaries between security and privacy concerns in DL and ML. These are the approaches that are being taken[17]. The DL and ML privacy technique with the greatest widespread use is called secure multiparty computing. Differential privacy is employed in this approach, which prevents an adversary from learning the use cases that were used in the construction of the target model (Aijaz Ali Khan, 2022) (D.G M. , 2019). Data used for training and testing is safeguarded against unauthorized access using a combination of secure multiparty processing and symmetric encryption[18]. Trusted execution environments take use of hardware-dependent security and isolation to protect sensitive data and training code. This helps ensure that the data and code remain safe. On the one hand, these techniques significantly increase the processing burden and need for a specialized method to be applied to each different kind of neural network.

Concerns about privacy in either the DL or ML domains have not been satisfactorily addressed in a way that is generally accepted. Many different security methods have been suggested as a means of providing defense against hostile assaults. These approaches may be classified into the following three categories: input processing, model resilience augmentation, and malware detection[19]. The objective of preprocessing is to lessen the reliance that the model has on data by carrying out processes like as image modification, randomization, and noise reduction. These are the kind of procedures that, in most cases, do not call for the model to be updated or retrained. The second category includes strategies such as regulation, trait reduction, adversarial training, and other methods to improve model stiffness via model retraining and modification[20]. This group also contains the approaches discussed in the first group. The detection of image transformations and adaptive noise reduction are two examples of third-scale detection techniques that may be applied prior to the first model layer. Another example would be the detection of a hidden layer. According to the best of our knowledge, there is no defensive strategy that can provide comprehensive protection against hostile situations (Dattatray G. Takale, 2022). despite the fact that a number of other defensive mechanisms have been suggested. Training against one's adversaries is presently the strategy that has shown to be the most successful in combating hostile circumstances. There are two primary means of protection against chemical assaults[21]. The first strategy is a selection approach called an odd selection, which eliminates anomalies from the relevant collection (Aijaz Ali Khan, 2022). In the second stage, you will try to increase the neural network's resilience to contamination caused by samples that are themselves tainted. In addition, a variety of studies on the Internet of Things applications and enhancements made possible by DL technology have been published in the relevant academic literature[22]. On the other hand, the majority of them tend to zero down on a particular facet of either DL or IoT. Take, for instance, a poll about the use of big data analytics to the Internet of Things. Furthermore take into consideration carrying out an analysis of the significant part that computer vision plays in the ground transportation system (D.G, 2019). This is not a thorough assessment that includes all recent research articles in the domains of IoT and learning; nevertheless, it does examine DL tendencies in the field of IoT. An important evaluation that is focused on enhancing IoT systems using DL has been carried out, however the majority of the attention is being paid to the duties of traffic scenario prediction and traffic sign recognition. Meeting the ever-evolving security requirements of the Internet of Things may be difficult since there are so many more linked devices than there were before. Solutions have to take into account the whole of the system in order to provide the requisite degree of safety. The majority of IoT devices, on the other hand, can function without the involvement of a human operator. When this occurs, unauthorized individuals are able to physically access these devices (Abomhara et., al., 2015)

Because privacy and security are inextricably linked, it is impossible to have privacy without security. Yet, security may exist independently of privacy. The availability, integrity, and confidentiality of information are all safeguarded by confidentiality, while the privacy of your personal information is more narrowly focused on only that aspect of your information. When it comes to the processing of personally identifiable information, protecting individuals' privacy is of the utmost importance; yet, information security is focused on restricting unauthorized access to various information sources. Any information that pertains to an individual may be considered personal data, such as their name, login information, address, social security number, bank account details, and so on. Other examples include. It is possible for more sophisticated and catastrophic attacks like Mirai to take place as a result of diverse IoT scenarios and applications. This is because IoT systems are susceptible to attack. Yet, it may be difficult to determine which security solutions are the most effective for Internet of Things devices. The data that is inputted into an Internet of Things system may be processed and aggregated to present conventional interface patterns, which enables early identification of criminal activities[21]. This article covers a variety of topics within the Internet of Things (IoT) sector, including but not limited to public transit, automobile sharing, vehicle identification, accident prediction, and inference. (Dr.Dattatray G. Takale, 2014). The goal of this paper is to make the subject matter included in it more in-depth and extensive. As a result, the objective of this article is to offer a comprehensive review of the most recent findings from research on Internet of Things (IoT) scanners for privacy and security, in addition to learning approaches[22]. Get more knowledge about Internet of Things and succeed in DL (Dattatray G. Takale S. S., 2022)

The broad use of IoT will directly lead to the deployment of IoT becoming a linked effort, which is a large and essential consequence as a direct outcome of the widespread application of IoT. 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 [22]. It is impossible to ignore one component when looking at developments in a different field [23]. This integration paves the way for academics working in fields that span various disciplines to investigate the challenges that are now faced by Internet of Things systems from a variety of perspectives, which opens up a new potential for them to do so. This integration does, however, bring forth additional security problems because of the dispersed nature of Internet of Things devices, which creates a large surface area that is susceptible to attack. These difficulties are a direct result of the increasing surface area, which is the root problem [24]. This characteristic of Internet of Things devices causes a great number of worries regarding users' personal safety and privacy. In addition to this, the platform for the Internet of Things generates a substantial amount of data that can be utilized. If these data are not analyzed and given in a secure setting, there is a substantial possibility that individuals' privacy will be compromised [25].

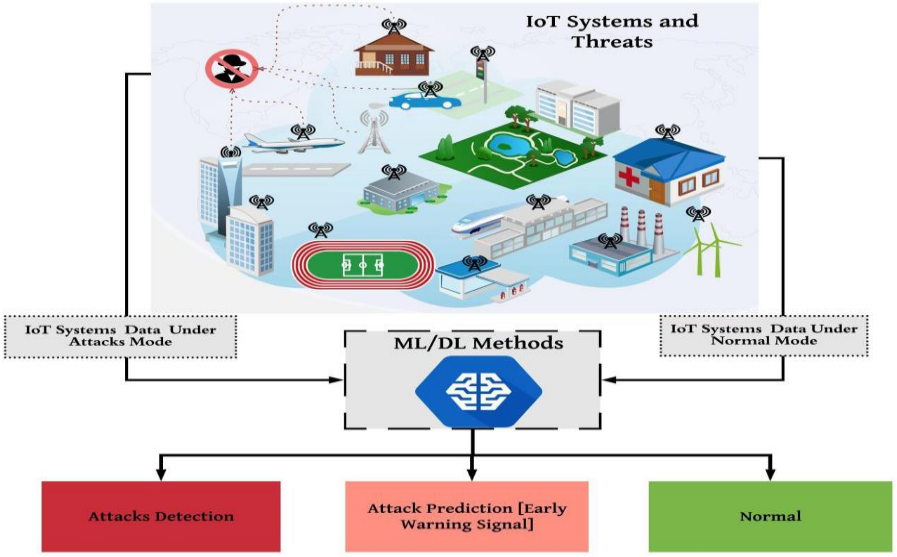
IoT Systems and Threats
IoT Systems Data Under Attacks Mode
ML/DL Methods
IoT Systems Data Under Normal Mode
Attacks Detection
Attack Prediction [Early Warning Signal]
Normal

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

As seen in Figure 1, having the ability to monitor IoT devices allows for the intelligent provision of a cure to new or zero-day attacks. If you want to find out what constitutes "normal" and "abnormal" behavior in terms of how components and devices of the internet of things interact with one another inside the internet of things ecosystem, you can use advanced data exploration techniques like machine learning and deep learning (ML/DL). Collecting and analyzing data from all IoT nodes allows us to identify anomalies in behavior and identify threats before they have a chance to spread. Due to its capacity to intelligently foresee future unknown assaults by learning from recent occurrences, ML and DL algorithms may be effective in forecasting new attacks, which are often mutations of earlier attempts. This is due to the fact that most modern assaults are only variants of previous ones. This means that in order for IoT systems to be trustworthy and secure, they will need to go beyond just facilitating secure communication between devices to providing security-based intelligence supported by deep learning and machine learning methods[19, 20].

2. LITERATURE REVIEW

In order to shed light on the state of IoT security and where the industry is headed, several researchers have conducted studies on the topic. His recent work on IoT security, however, focuses less on how ML and DL may be applied to the field. Encryption, authentication, access control, cyber security, and application security are all being discussed as potential weaknesses in IoT systems in recent studies. After discussing the issues and potential solutions related to IoT communications security, Kumar et al. (2017) zero in on that aspect of the system. The Internet of Things (IoT) has been the subject of several evaluations and research that aim to shed light on the potential threats that might arise in the future. IoT security has received a lot of attention, but there hasn't been any study on how to employ DL or ML to ensure the safety of IoT devices. Access control, authentication, application security, encryption, and cyber security were all areas that Kumar et al. (2017) felt needed improvement and regulation. Sfar et al. (2018) conducted research on the problems and potential solutions to securing IoT communications. Similar work was done by Zhao et al. (2013) on an Internet of Things intrusion detection system. Moreover, security and privacy needs may be defined by the IoT framework for regulatory approaches and regulatory concerns (Bengio et al., 2015). Privacy and security are integral parts of a distributed IoT infrastructure. There were a number of obstacles that dampened the effectiveness of this endeavor. Researchers think the dispersed IoT model provides various privacy and security advantages, but there are many concerns to address first.

Many traditional ML techniques, as well as cutting-edge approaches using DL for common huge data, were investigated. In order to analyze and explore relevant big data applications, a focus was placed on the coupling of various ML techniques with signal processing technologies. An in-depth analysis of contemporary methods for DL. The examination included the history and applications of several suggested solutions as well as their current open research problems. Several different DL models' underlying concepts were compared and contrasted, along with examples of how these models have been put to use and how far we've come in areas like computer vision, pattern recognition, and voice processing. For the benefit of mobile advertising, we surveyed the state of the art in DL for recommendation models. (Dattatray G. Takale S. S., 2022)

Moreover, self-organizing networks took use of a variety of effective machine learning strategies. The benefits and drawbacks of a number of approaches were examined, and recommendations for more research were offered. Together with the accompanying difficulties and opportunities, the future network topologies that contain AI were also taken into consideration. It was brought to everyone's attention how important AI is in a 5G environment. Data mining was discussed in both [1, 2] and [3, 4] with regard to the detection of network intrusions. It was also brought to everyone's attention that such applications bring their very own research challenges with them. In addition to that, there was an analysis of a multimedia mobile app that made use of DL. Current advancements in DL applications (G, 2019), such as state-of-the-art applications in speech recognition and language translation, mobile ambient intelligence and mobile security, mobile healthcare and mobile wellness, were some of the topics that were covered in this discussion. Comparable study was conducted on the most cutting-edge DL approaches that are currently being used for IoT data analytics across a variety of businesses.[19].

Diro and Chilamkurti [1] deep learning was explored as an unique intrusion detection tool for the Internet of Things setting, and the findings were encouraging. The authors also claimed that hundreds of zero-day attacks occur as a result of the inclusion of multiple protocols, the majority of which come from the internet of things (IoT). The majority of these zero-day assaults are tiny versions of cyber-attacks that were previously known. The occurrence of such a scenario demonstrated that even highly developed mechanisms, such as conventional machine-learning algorithms, have difficulties identifying tiny variants of assaults over the course of time.

Ramos et al. [2], provided a survey with a focus on quantitative security measures based on models, with the goal of determining how secure the complete network is. This study publishes a comprehensive literature review of the state of the art in Network Security Metrics (NSMs). The Common Vulnerability Scoring System (CVSS) framework is the major focus of the research since it feeds into so many other types of security metric models. The gaps between security metrics and related fields have also been the subject of study. More specifically for the field of model-based quantitative NSMs, this paper provides a thorough and extensive review of the primary measure proposals. As an added bonus, a detailed and extensive study of the primary measure concepts has been provided. All the major positives and negatives of the examined works have been included as well. At the end, a thorough evaluation of the key aspects of the security metrics under scrutiny was presented, along with a list of open issues and potential topics for further study. After this, a discussion on related prior work was held. With the data shown here, it is fair to argue that the field of model-based quantitative NSMs is in its infancy, and that much more work is needed to advance the field.

Granjal et al. [3] noted that users of other Internet infrastructures, including as cloud computing and most especially the IoT, whose security has received increased attention in recent years, would benefit from similar security measures.

Al-Fuqaha et al [4]. Challenges and issues related to IoT deployment strategy and execution, as well as IoT's relationship to big data analytics, cloud computing, and fog computing, were investigated. This research presents a revolutionary intelligent strategy for autonomous management, data aggregation, and protocol adaptation services. Improved horizontal integration amongst IoT services was the focus of this effort. They examined the IoT standards and protocols, spoke about how they work, and covered the many kinds of protocols and patterns that may be found in different parts of an IoT ecosystem. The authors also investigated the implications of IoT technologies like Big Data, cloud, and fog computing, and the need for a new generation of data analytics algorithms and tools with features like input size reduction that are tailored to IoT big data. Finally, this study concludes with a discussion of three applications that illustrate how the many protocols covered here may be combined to provide novel, intelligent Internet of Things services that give users access to previously unavailable features. The examples were provided.

Lopez-Martin et al [5], Introduced an innovative approach to network intrusion detection that was designed particularly for an Internet of Things network. The suggested approach makes use of a Conditional Variational

Auto encoder (CVAE) with a particular design that incorporates the intrusion labels into the decoder layers. This allows for the method to be implemented. In addition to being capable of performing feature reconstruction, the model that has been provided may also be used in the existing Network Intrusion Detection System, which is a component of network monitoring systems, and in particular in IoT networks. The suggested method only requires one training phase, which results in a significant reduction in the amount of computing resources required.

Fu et al [6], suggested that the Internet of Things would be a future component of 5G networks, but regrettably, the resources of IoT as devices are confined, and many security methods are hard to execute since the safety of IoT will undoubtedly be tied to many crucial scenarios of the future 5G. Regarding the extensive and diverse IoT networks, a strategy that is founded on the idea of automata has been offered in this piece of work. The technique employs an extension of Labelled Transition Systems to offer a standard definition of Internet of Things (IoT) systems that are able to identify intrusions by comparing the action flows of the various components.

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

Because of the distinctive way in which they tackle issues, learning algorithms have found widespread usage in a variety of applications that are based on the real world. The building of machines that improve themselves automatically via experience is handled by these sorts of algorithms. In recent years, learning algorithms have been put into effect in a variety of settings. The creation of novel algorithms and the availability of large amounts of data, in addition to the introduction of algorithms with cheap processing costs, have been driving forces behind the recent progress in the field of learning algorithms. From its inception as a curiosity in the laboratory, machine learning and deep learning have made considerable strides forward in recent years, becoming into operational equipment with a wide range of major applications [19]. Despite the fact that DL is a subfield of ML, the methods of ML that require engineered features are referred to in this paper. On the other hand, DL methods refer to recent advances in learning methods that utilize several non-linear processing layers for discriminative or generative feature extraction.

The primary means by which DT-based algorithms categorize data is by sorting samples in accordance with the feature values they possess. A tree's vertices, also known as nodes, each represent a feature, and the tree's branches, also known as edges, each imply a value that a vertex in a sample being classed may have. The samples are categorized using the origin vertex as the starting point and with according to the feature values they possess. The origin vertex of the tree is determined to be the feature that separates the training samples in the most effective manner [16]. The information gain [17] and the Gini index [17] are two of the variables that are used in the process of determining the ideal feature that most effectively separates the training samples.

The probability of an occurrence is explained by Bayes' theorem [18], which takes into account prior information about that event. You may look up Bayes' theorem on this page. For instance, network traffic data is used to spot DDoS attacks. Bayes' theorem is one approach to estimate the likelihood of network traffic being linked to an attack (or not related to an attack) by utilizing information about past traffic. A common machine learning approach, the Naive Bayes (NB) classifier [18] is based on Bayes' theorem.

The NB classifier is a commonly used supervised classifier known for its simplicity. NB calculates posterior probability and uses Bayes' theorem to forecast the probability that a particular feature set of unlabeled examples fits a specific label with the assumption of independence amongst the features[19]. For example, for intrusion detection, NB can be used to classify the traffic as normal or abnormal. The features that can be used for traffic classification, such as connection duration, connection protocol (e.g. TCP and UDP) and connection status flag, are treated by the NB classifier independently despite that these features may depend on one another. In NB classification, all features individually contribute to the probability that the traffic is normal or abnormal; thus, the modifier "naïve" is used. NB have been used for network intrusion detection [20,21] and anomaly detection [20, 21]. The main advantages of NB classifiers include simplicity, ease of implementation, applicability to binary and multi-class classification, low training sample requirement[23] and robustness to irrelevant features (The features are preserved independently.). However, NB classifiers cannot capture useful clues from the relationships and interactions among features (Dattatray G. Takale S. U., 2022). The interactions among features can be important for accurate classification, particularly in complex tasks in which the interactions among features can significantly help the classifier increase its discrimination power among classes [24].

The KNN approach is one that does not rely on parameters. The Euclidean distance is often the distance metric that is used by KNN classifiers [19]. The KNN classification method is shown in Figure 6, which shows how fresh input samples are categorized. The behaviors shown by the red circles in the picture are considered to be malevolent, while the behaviors depicted by the green circles are considered to be typical of the system. The previously unidentified sample, shown by the blue circle, needs to be categorized as either malevolent or typical behavior. The KNN classifier assigns a category to a new example based on the votes cast by a certain number of its closest neighbors; in other words, the KNN algorithm determines the category of unknown samples based on the vote that receives the most support from its neighbors. For example, in Figure 6, if the KNN classification is based on the behavior of one closest neighbor (k = 1), then it will categorize the class of the unseen sample as normal behavior (Dattatray G. Takale R. R., 2022). If the KNN classification is based on two nearest neighbors (k = 2), then the KNN classifier will categorize the class of the unseen sample as normal behavior since the two circles that are geographically closest to it are green (normal behavior). If the KNN classification is based on three and four nearest neighbours (k = 3, k = 4), then the KNN classifier will categorize the class of the unknown sample as malevolent conduct since all of the three and four circles that are closest to it are red (malicious behavior). The process of cross-validation is an essential step in determining the value of k that yields the best results for a particular dataset. One of the steps in this process involves testing many k-values. Despite the fact that the KNN method is a straightforward classification technique that works well with big training datasets [19], the optimal value for k will always be different depending on the datasets [20]. As a result, obtaining the value of k that is ideal may be a procedure that is difficult and time-consuming.

The RFs are types of learning algorithms known as supervised learning. In an RF, many DTs are built and then integrated in order to gain an accurate and reliable prediction model for the purpose of achieving superior overall outcomes [23]. Hence, an RF is made up of a great number of trees that are built in a random order and are taught to vote for a certain class. The ultimate result of categorization is determined to be the category that received the most votes [24]. These two classification methods are quite different from one another, in spite of the fact that the RF classifier is built mostly utilizing DTs. Initially, when the training set is introduced into a DT network, the network will typically generate a set of rules, which will then be used to categorize any new inputs that are introduced into the network. RF is resistant to over fitting because it employs decision trees (DTs) to generate subsets of rules for voting on a class. As a consequence, the classification output is the average of the outcomes, and RF is efficient. In addition to this, feature selection may be skipped using RF, and it only needs a few input parameters [24]. Nevertheless, since RF requires the building of numerous DTs, its implementation may be difficult in some real-time applications in which a large training dataset is needed.

This is because RF has to train its models using several datasets. In order to identify network anomalies and intrusions, radio frequency (RF) techniques have been used. RF, SVM, KNN, and ANN were trained to detect DDoS in IoT systems in a previous study. When limited feature sets were used to avoid additional computational overhead and improve the applicability of the system to real-time classification, RF provided slightly better classification results than did the other classifiers. (Dattatray G. Takale R. R., 2022).

4. CONCLUSION

Since many technologies, ranging from physical devices and wireless connections to mobile and cloud architectures, need to be safeguarded and integrated with one another, the security requirements for devices connected to the internet of things are getting more complicated. Some strong analytics tools that may be used to enhance the security of the internet of things have been produced as a result of advancements in machine learning and deep learning. This research investigates a variety of risks to the Internet of Things (IoT) as well as IoT attack surfaces (Dattatray G. Takale S. D., 2022). This article presents a thorough review of the ways in which ML and DL techniques may be used to Internet of Things (IoT) security. After that, we evaluate the benefits and drawbacks of various technologies and how they might be used to protecting the Internet of Things (IoT). Next, we take a look at the machine learning and deep learning techniques that make the underlying IoT layers possible (i.e. knowledge, network, and application layers). In a nutshell, there has been a great deal of research conducted with a great number of DL models in a variety of IoT domains; nevertheless, there are still a great deal of issues, hurdles, and potential future directions in the application of DL. Be sure you utilize DL. Make efficient use of machine learning and deep learning to protect managed, categorized, and secure IoT systems. Teaching tactics, including how to design strong detection models, how to assure security and privacy via models, and how to develop deep learning models that effectively make use of the produced heterogeneous IoT data [24].

Lastly, machine learning and deep learning for Internet of Things security in an interactive, networked, and interdependent environment of IoT systems; certain security trade-offs in IoT applications; and simultaneous integration of ML and DL with block chain for Internet of Things security. This study intends to give a helpful guide that may motivate researchers to enhance the security of Internet of Things (IoT) systems. This improvement can range from merely allowing secure communication between IoT components to establishing end-to-end intelligent IoT development [25].

The research report arrives to the conclusion that deep learning and machine learning algorithms have just been created in recent years and are not designed to be used in cryptographic applications. Cryptography may, however, be implemented using machine learning and deep learning by researchers who are capable of doing cryptography. In a similar vein, Alaba (2017) demonstrated how DL algorithms can decipher cipher frames and came to the conclusion that they can. CNN and AE algorithms have mostly supplanted the machine learning algorithms and logical processes that were previously used. It has been shown that RNNs are capable of learning to decode the information they are fed. The successful analysis of the internal representations of this encoder may also be utilized to decode fuzzy machine data on RNNs by using a three thousand-unit long short-term memory (LSTM) network. The findings of the systematic review conducted for this study reveal, among other things, that deep learning algorithms such as RNN are able to discover and analyte polyalphabetic ciphers for the purpose of cryptanalysis. Research in machine learning and deep learning has the potential to speed up the development of the Internet of Things. It is vital to protect the endpoints of these devices since a significant number of intelligent objects are linked to devices that are part of the internet of things. On the other hand, the dependable advantages of IoT DL models are outlined, as are major areas for the development of IoT DL research in the future.

REFERENCES

1. A.A. Diro, N. Chilamkurti, Distributed attack detection scheme using deep learning approach for internet of things, Future Gener. Comput. Syst. 82 (2018) 761–768. [Online]. Available: http://www.sciencedirect.com/science/article/pii/ S0167739X17308488.

2. A. Ramos, M. Lazar, R.H. Filho, J.J.P.C. Rodrigues, Model-based quantitative network security metrics: a survey, IEEE Commun. Surv. Tut. 19 (4) (2017) 2704–2734. [Online]. Available: http://www.sciencedirect.com/science/article/ pii/S0167739X17308488.

3. J. Granjal, E. Monteiro, J.S. Silva, Security for the internet of things: a survey of existing protocols and open research issues, IEEE Commun. Surv. Tut. 17 (3) (2015) 1294–1312 [Online]. Available, doi:10.1109/comst.2015.2388550.

4. 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.

5. 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.

6. R.K. Gunupudi, M. Nimmala, N. Gugulothu, S.R. Gali, Clapp: a self constructing feature clustering approach for anomaly detection, Future Gener. Comput. Syst. 74 (2017) 417–429. [Online]. Available: http://www.sciencedirect.com/science/ article/pii/S0167739X16308718.

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

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

9. Ray,S.Y.Jin,andA.Raychowdhury,(2016)“Changingcomputingparadigmwithinternetofthings:atutoriali ntroduction,”IEEEDesign&Test,vol.33,no.2,pp.76–96,2016.

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

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

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

13. Sicari,S.A.Rizzardi,L.A.Grieco,andA.CoenPorisini,(2015).“Security,privacyandtrustinInternetofThing s:Theroadahead,”Comput.Netw.,vol.76,pp.146–164,Jan.2015.

14. Alaba,F.A,M.Othman,I.A.T.Hashem,andF.Alotaibi,(2017).“InternetofThingssecurity:Asurvey,”J.Netw .Comput.Appl.,vol.88,pp.10–28,Jun.2017

15. AA Khan, RM Mulajkar, VN Khan, SK Sonkar, DG Takale. (2022). A Research on Efficient Spam Detection Technique for IOT Devices Using Machine Learning. NeuroQuantology, 20(18), 625-631.

16. SU Kadam, VM Dhede, VN Khan, A Raj, DG Takale. (2022). Machine Learning Methode for Automatic Potato Disease Detection. NeuroQuantology, 20(16), 2102-2106.

17. DG Takale, Shubhangi D. Gunjal, VN Khan, Atul Raj, Satish N. Gujar. (2022). Road Accident Prediction Model Using Data Mining Techniques. NeuroQuantology, 20(16), 2904-2101.

18. SS Bere, GP Shukla, VN Khan, AM Shah, DG Takale. (2022). Analysis Of Students Performance Prediction in Online Courses Using Machine Learning Algorithms. NeuroQuantology, 20(12), 13-19.

19. R Raut, Y Borole, S Patil, VN Khan, DG Takale. (2022). Skin Disease Classification Using Machine Learning Algorithms. NeuroQuantology, 20(10), 9624-9629.

20. SU Kadam, A katri, VN Khan, A Singh, DG Takale, DS. Galhe (2022). Improve The Performance Of Non-Intrusive Speech Quality Assessment Using Machine Learning Algorithms. NeuroQuantology, 20(19), 3243-3250.

21. DG Takale, (2019). A Review on Implementing Energy Efficient clustering protocol for Wireless sensor Network. Journal of Emerging Technologies and Innovative Research (JETIR), Volume 6(Issue 1), 310-315.

22. DG Takale. (2019). A Review on QoS Aware Routing Protocols for Wireless Sensor Networks. International Journal of Emerging Technologies and Innovative Research, Volume 6(Issue 1), 316-320.

23. DG Takale (2019). A Review on Wireless Sensor Network: its Applications and challenges. Journal of Emerging Technologies and Innovative Research (JETIR), Volume 6(Issue 1), 222-226.

24. DG Takale, et. al (May 2019). Load Balancing Energy Efficient Protocol for Wireless Sensor Network. International Journal of Research and Analytical Reviews (IJRAR), 153-158.

25. DG Takale et.al (2014). A Study of Fault Management Algorithm and Recover the Faulty Node Using the FNR Algorithms for Wireless Sensor Network. International Journal of Engineering Research and General Science, Volume 2(Issue 6), 590-595.

26. DG Takale, (2019). A Review on Data Centric Routing for Wireless sensor Network. Journal of Emerging Technologies and Innovative Research (JETIR), Volume 6(Issue 1), 304-309.

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