Materials Today: Proceedings 80 (2023) 2518–2523

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

Identification of cyber attacks using machine learning in smart IoT networks

C. Malathi [a,*], I. Naga Padmaja [b]

[a] Department of Computer Science, Sri Padmavathi Mahila Visvavidyalayam, Tirupati, AP, India
[b] Department of Information Technology RVR&JC College of Engineering, Chowdavaram, Guntur, AP, India

ARTICLE INFO

Article history:
Available online 28 July 2021

Keywords:
Network abnormal detection
Machine-learning (ML)
Internet of Things (IoT)
Cyber attacks
BoT-IoT metadata
Cyber security

ABSTRACT

The Internet of Things (IoT) combines billions of physical objects that can communicate with each device without minimal human interaction. IoT has grown to be one of the most popular technologies and an attractive field of interest in the business world. The demand and usage of IoT are expanding rapidly. Several organizations are funding in this domain for their business use and giving it as a service for other organizations. The result of IoT development is the rise of different security difficulties to both organizations and buyers. Cyber Security gives excellent services to preserve internet privacy and business interventions such as disguising communication intrusions, denial of service interventions, blocked, and unauthorized real-time communication. Performing safety measures, such as authentication, encryption, network protection, access power, and application protection to IoT devices and their natural vulnerabilities are less effective. Therefore, security should improve to protect the IoT ecosystem efficiently. Machine Learning algorithms are proposed to secure the data from cyber security risks. Machine-learning algorithms that can apply in different ways to limit and identify the outbreaks and security gaps in networks. The main goal of this article ability to understand the efficiency of machine learning (ML) algorithms in opposing Network-related cyber security Assault, with a focus on Denial of Service (DoS) attacks. We also address the difficulties that require to be discussed to implement these Machine Learning (ML) security schemes in practical physical object (IoT) systems. In this research, our main aim is to provide security by multiple machine-learning (ML) algorithms that are mostly used to recognise the interrelated (IoT) network Assault immediately. Unique metadata, Bot-IoT, is accustomed to estimate different recognition algorithms. In this execution stage, several kinds of Machine-Learning (ML) algorithms were handled and mostly reached extraordinary achievement. Novel factors were gathered from the Bot-IoT metadata while implementation and the latest features contributed more reliable outcomes.

Selection and peer-review under responsibility of the scientific committee of the International Conference on Nanoelectronics, Nanophotonics, Nanomaterials, Nanobioscience & Nanotechnology.

1. Introduction

In recent years, the generation of IoT has been broadly growing completely in the real world. Concerns about safety and privacy about networks are growing in the present moment, and system safety measures have grown a specification as a development of the extent of data technology in day-to-day life [1]. The advance in several Internet applications and the development of advanced technology like the practical physical object (IoT) systems is succeeded by fresh efforts to attack machine networks and computer system. The practical physical object (IoT) is a collection of inter related objects where smart machines are connected without the requirement of human mediation. Several smart IoT devices have sensors that can connect to the internet to share information from one node to another like healthcare applications, farming applications, transportation applications, and many others. IoT devices are used to save time and resources and change the work style. It also has countless benefits and many possibilities for the transfer of information, modification, and extension. Each safety threat is present within the internet together with in IoT for the reason that cyberspace is the center and core of the practical physical object systems i.e IoT. Related to the additional conventional net, practical physical object systems junctions obtain less capability

* Corresponding author.
E-mail address: malathichakravarthula@gmail.com (C. Malathi).

https://doi.org/10.1016/j.matpr.2021.06.400
2214-7853/
Selection and peer-review under responsibility of the scientific committee of the International Conference on Nanoelectronics, Nanophotonics, Nanomaterials, Nanobioscience & Nanotechnology.

and insufficient assets and restrictions of manual commands. Moreover, with the fast advance of IoT smart devices adoption in daily life, so IoT security issues are very difficult to find, cyber security is required to implement safety solutions based on networks. Modern techniques are used to detect some cyber attacks, it is a more challenging issue to find other cyber attacks. As network cyber-attacks increase, along with a large volume of the report present in computer networks, extra active and more efficient techniques are required for the detection of cyber attacks and no doubt at all that there is a lot of chance to improve network safety. In this situation, Machine Learning algorithms implement secured intelligence in the IoT Network, Machine Learning (ML) is considered as the most powerful computational model. Machine learning (ML) methods are used for several network security responsibilities like intrusion detection, network traffic analysis, and bot-net recognition.

Machine-Learning (ML) might be defined as a knowledgeable smart device's capability to change a knowledgeable behaviour and state of the device, which is granted a crucial portion of the practical physical object system solution. Machine Learning (ML) can understand valuable information of data produced by machines and people, and Machine Learning algorithms may be used in many tasks such as classification and regression. Moreover, Machine Learning (ML) is used to provide security services in an IoT network. ML used in cyber attack detection difficulties is growing a hot topic, and Machine Learning (ML) can be used in various prosecution in the cyber-security field. Assuming several kinds of research in the summary became used Machine-Learning (ML) methods to identify the most reliable methods to identify offensive, individual poor groundwork exists on effective detection techniques advisable for practical physical object system environments.

Machine-Learning (ML) might be utilized for cyber attack recognition assignment through two principal types of cyber-analysis: misuse allotted technique [6], signature allotted technique or anomaly allotted technique. misuse allotted methods are planned to identify well-known cyber-attacks by applying particular cyber traffic properties; it is also defined as "signatures" in such latest cyber-attacks. Detection methods contain many benefits: that capability to recognize identified cyber attacks completely with no creating a powerful amount of wrong signals. In the article, a few professions handling signature allotted methods for identifying cyber attacks; for example, Area of traffic analysis used various ML methods as preceding devices to study the characteristics of any known cyber attacks. Signature-based methods can be used in compromised machines to detect by using botnet traffic instructions. The major disadvantages of signature-based strategies are that the effective performance of certain strategies needs regular standard updates of cyber-attack traffic indications and that certain procedures cannot catch earlier anonymous aggression. The next level of identification techniques is anomaly allotted recognition. The strength of the section is to identify anonymous cyberattacks that make them engaging to handle. The crucial problem along anomaly allotted methods are feasible of huge fake signal rates (FSRs), as before unfamiliar behaviors can be viewed as irregularities. Anomaly and Signature detection methods can be merged as heterogeneous methods. One of the heterogeneous method samples is exhibited wherever this method is utilized to improve the exposure amount of known cyberattacks or decrease fake positive (FP) amount for anonymous cyberattacks.

Our research provides a report incorporated with defense against practical physical object system cyber-attack behaviour through examining the efficiency of machine- learning (ML) methods to identify practical physical object network cyber-attacks. Most of the ML identification algorithms can be estimated using a Bot-IoT, current metadata that merges authentic and fabricated practical physical object cyber traffic with many kinds of cyberattacks. Characteristics are elected from this dataset by managing the Random Forest Regressor (RFR) algorithm. In this implementation stage, seven various Machine-Learning (ML) algorithms have huge performance and are used frequently. The following algorithms are used in Machine-Learning: Random Forest, K-nearest neighbours (KNN), Quadratic discriminant analysis (QDA), ID3 (Iterative Dichotomiser, AdaBoost, Naıve Bayes (NB), and Multilayer perceptron (MLP).

This legacy can be reviewed through this analysis as:

- Amendment in offence discovery and practical physical object networks through assessing an execution of Machine-Learning (ML) algorithms on a current practical physical object metadata.
- Remove distinct characteristics in metadata and choose the most common relevant characteristics to develop the performance of Machine-Learning (ML) algorithm.

2. Literature review

The area of expert systems has been broadly investigated, and numerous academic articles about interference exposure by Knowledge Discovery (KD) methods and computer knowledge advertised but few of these preceding studies contain a lot of Machine-Learning (ML) for interference discovery in conventional networks. We are consequently enlarging this field of experimentation in this research by especially using Machine Learning (ML) to identify cyberattacks in the practical physical object. The importance of expert system methods to the practical physical object field exists in the beginning stages of research, specifically in data and smart device security becomes a huge opportunity to find insights from smart devices data or practical physical object systems. Some of smart combined networks, Machine-Learning (ML) policies such as anomaly detection, pattern recognition, and behavioural analysis would be utilized to recognize possible cyberattacks, prevent unusual behaviours. To evaluate the modern analysis of cyberattack utilising Machine-Learning (ML) in practical physical object networks, explored different investigations and reviewed them. Every research, machine learning(ML) algorithms, detection approaches, and datasets are supplied. While choosing those studies, we concentrated on the performance of various datasets and machine learning (ML) algorithms. The investigations contribute proof that machine learning (ML) methods can attain achievement for intrusion detection. the effect of machine learning for IoT protection from the work addressing, the detection approaches can be classified as unsupervised techniques and supervised techniques.

Several types of research should preferable that Machine-Learning (ML) methods could be used to assist cyberattack identification containing artificial neural networks (ANNs), k-means, auto-encoder, Random Forest (RF) and Many scholars use unsupervised algorithms for identification difficulties [16]. Auto encoders are the significant unsupervised ML algorithms that are used in several works; for instance, Mirsky et al. [10] suggested auto-encoders are used to remove characteristics from datasets to develop the identification of cyberattacks. They launched Kitsune [11], An unsupervised interruption detection method that can acquire for identify cyber-attacks on cyber networks effectively. Kitsune's major procedure uses a collection of neural networks (NN), also called auto-encoders, to differentiate between anomalous and normal traffic patterns. In [12], Meidan et al. introduced and estimated a unique identification system that removes behavioural snaps of the network and also applies auto-encoders to identify abnormal network traffic of yielded things. The main disadvantage of unsupervised machine learning (ML) procedure for identification difficulties in the network, highest anomalies and

normal cyberattacks, outliers are few, which asymmetrically influence the rate of success and the identification of irregularities. More reliable outcomes are required with supervised methods for that purpose. Supervised Machine learning (ML) algorithms are utilized to identify cyberattacks and instructed on metadata including labels intimating whether the examples have been pre-classified as cyberattacks. In [19], Elike and Hodo utilized a Support-Vector-Machine (SVM) and Artificial Neural Networks (ANN) and algorithms, these are used to identify non-Tor traffic cyber attacks on UNBCIC datasets by applying Machine learning (ML) methods. To explicitly classify IoT smart device models of the whitelist In [15], the Random Forest (RF) algorithm was implemented to characteristics derived from network traffic information. In Proposed work [13], use the related Bot-IoT metadata and concentrate on extorting highlights of the metadata and estimating various Machine-Learning (ML) algorithms on the Bot-IoT metadata.

The Self-Normalizing Neural Network achievement compared with Feedforward Neural Network for analyzing unwanted aggression in a practical physical object network. Depending on various special grades in certain tests, the Feedforward Neural Network (FNN) exceeded Self-normalizing Neural Network (SNN) in their laboratory outcomes for unwanted detection in practical physical object networks. Ferrag, in [14], uses the Bot-IoT metadata for estimate the Deep-Coin architecture representation in the amount of data moving across a computer network produced by smart device networks. Deep-Coin is an unique blockchain-based energy framework and deep learning framework. by utilizing the Bot-IoT dataset by performance evaluations, they described the advanced performance of the Deep-Coin framework [1718].

3. Proposed approach

This segment presents a little summary of the metadata used and the advanced method to identify cyberattacks in physical and wireless networks. In the advanced strategy, several original and pre-processing applications are implemented to recognize irregularities by using machine learning (ML) methods. Primary, flow-based highlights of the natural metadata were excerpted by CIC Flow-Meter. In the initial step, the information initialisation method is implemented before splitting the dataset into two segments: training and test segments. Data pre-processing is needed to convert the information within a suitable pattern by using Machine-Learning (ML) algorithms. Later in certain processes, the attributes being performed by the ML methods are determined in the attribute modification level. Ultimately, the proposed strategy concludes the implementation of Machine-Learning (ML) procedures. An outline of the advanced strategy is shown in Figs. 1 and 2.

The Bot-IoT metadata is the best dataset for the experiments because of wide attack diversity, regular updates, the capability to make distinct points from the fresh dataset, and the addition of IoT-generated network traffic. The Bot-IoT metadata was generated in the Cyber Range Lab at the Australian Centre for Cyber Security (ACCS). Bot-IoT metadata contains triply types of cyber attacks just like DoS, Probing, and Data Theft. CIC Flow-Meter is used to remove origin-based highlights of fresh network traffic tracks. CIC Flow-Meter is a web traffic flow dynamo shared by CIC to form 84 data move out features.

4. Implementation

As we have discussed in the foregoing section, the primary goal of the experiment is to decide the Machine-Learning achievement in identifying physical objects incursion. This segment defines the BoT-IoT metadata, machine learning (ML) mechanism used in our implementation steps.

4.1. Datasets or metadata

The dataset is a collection of information that is prescribed as an individual unit by a machine. This indicates that a dataset holds a lot of separate bits of data but that can be used to instruct an algorithm to detect expected patterns inside the entire dataset. The applications use machine learning (ML) techniques for different network cyber security, massive metadata are required to examine data network traffic flows and differentiate among normal and abnormal network traffic. For instance, in [12], Meidan et al. formed an openly accessible practical physical object metadata specified as N-BaIoT, and multiple kinds of research adopted metadata for education and for experiment with classifier examples. Metadata is almost huge, clear and unstable, the degree of natural information extremely weak related to cyber-attack information. Moustafa et al. [9] attempted to discuss the weaknesses by creating the Bot-IoT metadata. The Bot-IoT metadata consolidates authentic, fabricated web traffic with several kinds of cyber attacks. The BotIoT data archive cyber attacks are categorized as triply kinds: information theft, DoS, Probing incursion.

4.2. Machine Learning algorithms

ML techniques are utilized the Bot-IoT dataset to estimate seven (7) well-known Machine-Learning (ML) classifiers: Random Forest, Iterative Dichotomiser 3 (ID3), K-Nearest Neighbours (KNN), AdaBoost, Multilayer perceptron(MLP), Naıve Bayes (NB) classifier, and Quadratic discriminant analysis. While preferring those classifiers, the focus is on inducing unitedly famous algorithms with various features.

- K-Nearest Neighbours: It is the easiest as well as most powerful supervised Machine Learning (ML) algorithm. It has been done for exploring throughout the possible metadata to incorporate distinct information with related existing data.
- Quadratic discriminant analysis (QDA): It is the perfect method for supervised classification difficulties. QDA exists a mathematical method to allow systematic information for a single group between multiple groups.
- Iterative Dichotomiser 3(ID3): this method is utilized to build a flowchart from a metadata. ID3 is typically used in Natural Language Processing (NLP) and Machine Learning (ML) domains.
- Random Forest (RF): The common purpose of random forests was introduced by Ho in 1995. RF is a method that utilizes flowchart. In this process, a “forest” is constructed by gathering a huge amount of various structures that are developed in various methods[28]. This algorithm consists of several benefits, like the capacity to run on large datasets, less load correlated to various systems and strength in opposition to noise and observation when matched to individual classifiers.
- Adaptive Boosting: it concentrates on classification problems, attempts to change ineffective classifiers into effective classifiers. It can be associated with several different varieties of Machine Learning (ML) algorithms to enhance achievement.
- Multilayer Perceptron (MLP): Multilayer Perceptron is a level of feed-forward ANN. ANN is Machine-Learning(ML) classification that catches motivation out from the process of people’s intellect tasks, like training and obtaining further knowledge.
- Naive Bayes(NB): The Naive Bayes(NB) is a broadly adopted supervised machine learning (ML) approach, as well as being more popular for its easy policies. The NB approach depends

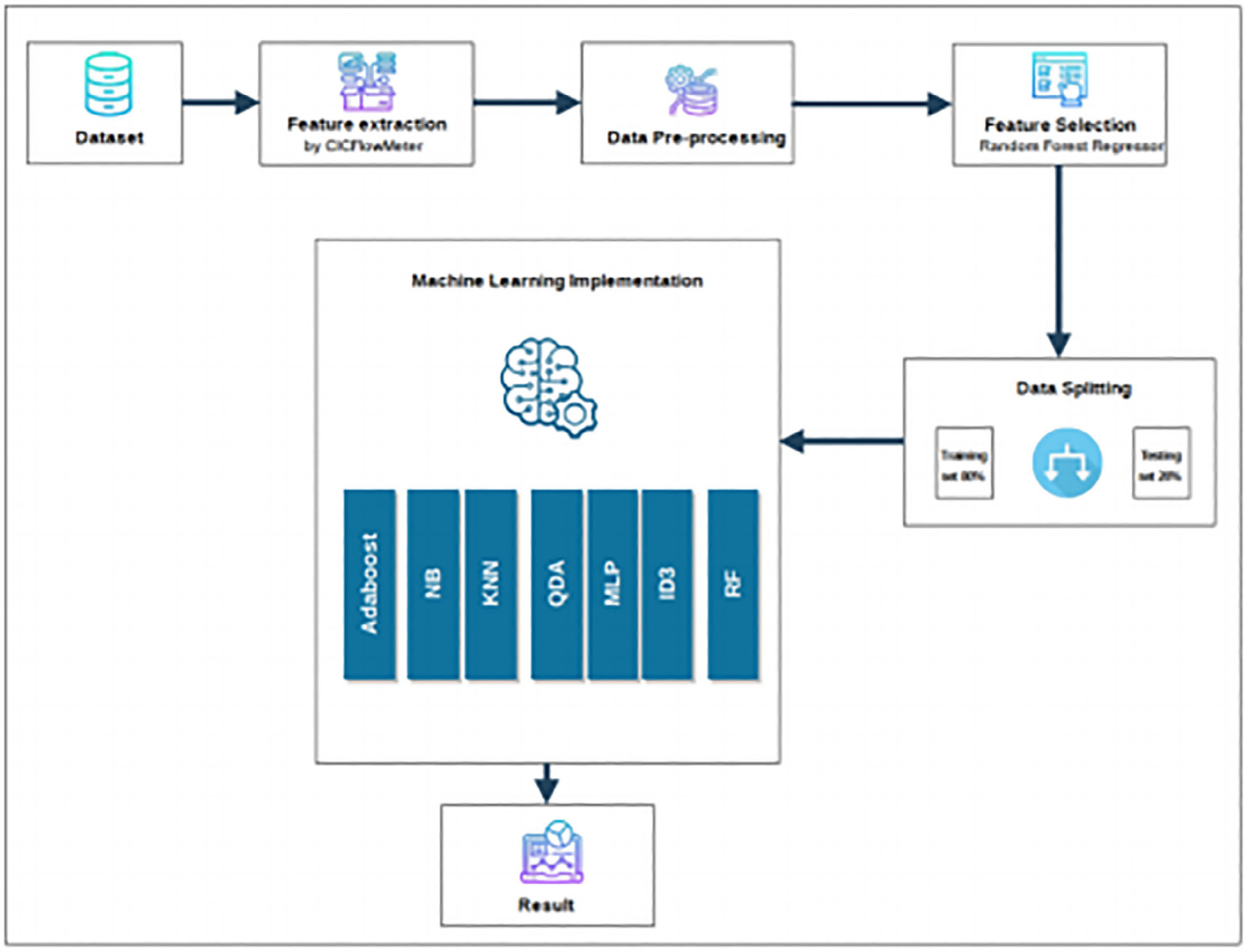

Fig. 1. Proposed Overview Strategy.

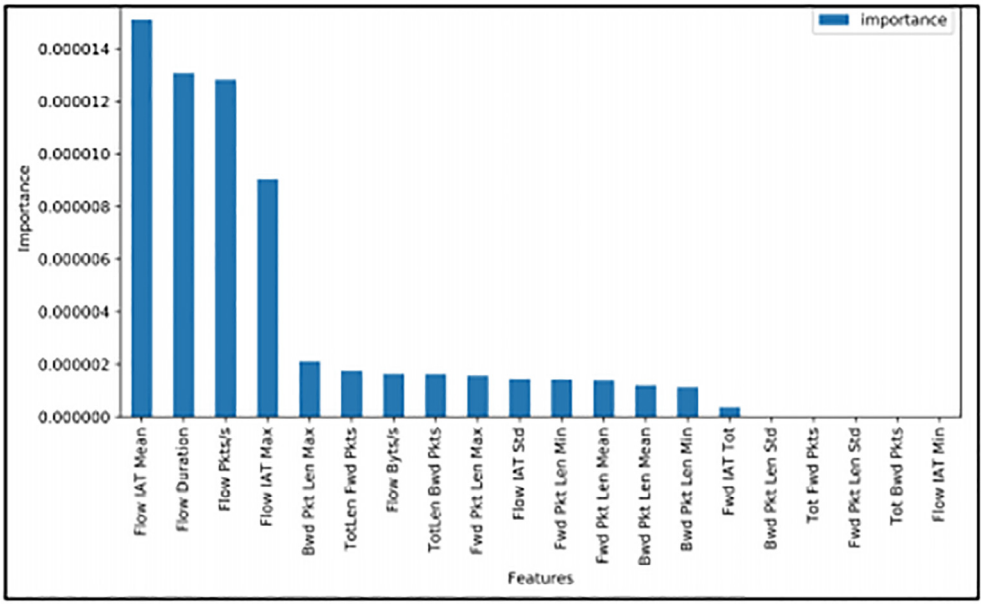

Fig. 2. Graph of complete dataset importance.

on the performance of Thomas Bayes. For example, Naive Bayes (NB) would be employed to classify network data transfer as normal or anomalous for unknown identification. The network data distribution characteristics are managed individually through Naive Bayes classifier even though certain characteristics may depend on each other.

4.3. Implementation steps

Our proposed system contains 5 steps of fundamental methods: Splitting data, data pre-processing, Feature extraction, feature selection, and implementation of Machine-Learning algorithms (ML).

- Feature Extraction: CIC Flow-Meter is used to reduce the flow-based characteristics out from new web distribution information. CIC Flow-Meter exists web data traffic spread by CIC Flow-Meter that provides eighty four(84) web traffic features. It presents the pcap record, gives a visible record of the characteristics obtained, and more grants a Excel CSV file of the metadata.
- Data preprocessing: is a Machine Learning technique that involves converting raw information into a readable format. Data cleaning and conversion are techniques applied to eliminate outliers and normalize the information so that they need a pattern that can be efficiently utilized to build a design.
- Splitting Data: Data is divided into different categories using Machine Learning (ML) methods. It is also required for training and tests to judge the efficiency of ML approaches. In our research, we analyzed 84% of the Bot-IoT metadata for the training data as well as the remaining 16% for the testing data.
- Feature selection: it is the method of decreasing the number of input variables when growing a predictive paradigm. It uses the characteristics required to test and train the approaches to detect a less weight protection resolution suitable for IoT network systems.
- Machine-Learning(ML) Approaches & Implementations: the complete execution is implemented in PYTHON and JAVA by applying Machine-Learning(ML) Libraries such as Matplotlib, scikit-learn, NumPy, and Pandas.
- Machine-Learning(ML) algorithms are designed for the metadata in 3 stages: 1) employing the advanced approach on every cyber-attacks independently; 2) employing the various ML approaches on the complete metadata with a collection of characteristics joining the most suitable characteristics for a specific cyber-attack and employing the ML approaches on the complete metadata with the 7 most desirable characteristics acquired in the background collection step.

5. Evaluation

A. Evaluation Metrics: While estimating the completion of ML standards, it is essential to determine completion models for the responsibility. To estimate decisions metrics, the most critical performance notices are used for the correctness, efficiency, f-measure, and recall, as explained in the mathematically here:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{2}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{3}$$

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN} \tag{4}$$

$$\text{F} - \text{measure} = \frac{2}{\frac{1}{Recall} + \frac{1}{Precision}} \tag{5}$$

5.1. Results

As declared in the earlier segment, we designed the ML approaches evaluation for the metadata in 3 stages.

Stage 1: employing ML Techniques on every cyber-attacks in the metadata independently; Stage 2: employing ML Techniques on the complete dataset; and Stage 3: employing ML Techniques on the complete metadata with a couple of the most useful characteristics for every cyber-attacks with 7 characteristics.

- Phase 1: ML procedures work on every cyber-attack in the metadata independently. Various ML techniques are employed for ten various cyber attacks. The events of the ML procedure, if there is an equivalence in the F-measure, the following conditions are considered to reduce identity: precision, accuracy, recall, and time.
- Phase 2: ML procedures employing on the complete metadata with a collection of characteristics merged with the most useful characteristics for every cyber-attacks. Several various techniques of ML were performed on the complete metadata, and adopted property sets that are selected for every cyber assault independently.
- Phase 3: employing ML methods on the complete metadata with the several most useful characteristics acquired in the peculiarity determination stage. From the F-measure prospect, there is no notable difference in ML procedure appearance, but from the prospect, the functioning times of complete ML methods were decreased.

The ultimate outcomes of the implementation are associated with research in the paper. Toward this observation, the research conveyed by Ferrag et al. was preferred in 2019. The purpose for specified work adopted the identical dataset as well as a couple of machine learning (ML) techniques related to the items. Those similar ML approaches are Naive Bayes (NB) and Random Forest (RF). The fundamental key separation between work and the property collection is done. They adopted the primary property collection while adopting a unique property collection selected by CIC FLOW-METER.

6. Conclusion

This article intended to identify web attacks by using ML techniques. In these circumstances, Bot-IoT was employed as a metadata because of its frequent refurbish, different network rules, and broad cyber attack differences. We adopted CIC Flow-Meter to remove flow-based innovations of the new network's traffic spots. CIC Flow-Meter produces 94 web traffic characteristics of the metadata that determine the web data flow. For the time of implementation, the value of power estimates was done with the Random Forest Regressor (RFR) method to determine which of the specialties might be applied in the ML techniques. A couple of approaches were utilized when performing those estimates. In the primary procedure, the value of measurements was computed distinctly for every cyberattack model, and in the secondary procedure, all the cyberattacks were obtained in a particular combination and the value of measurements for this combination is determined; i.e., the natural resources are essential for total every intrusions defined. Eventually, Several ML techniques that are extensively utilized and contain several properties are connected for that information.

CRediT authorship contribution statement

C. Malathi: Conceptualization, Methodology, Data curation, Writing - review & editing. **I. Naga Padmaja:** Visualization, Investigation, Validation, Writing - original draft, Supervision.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] J. Deogirikar and A. Vidhate, "Security attacks in iot: A survey," International Conference on I-SMAC (I-SMAC), pp. 32–37, 2017.
[6] I. Lambert and M. Glenn, "Security analytics: Using deep learning to detect cyber attacks," 2017.
[9] Nickolaos Koroniotis, Nour Moustafa, Elena Sitnikova, Benjamin Turnbull, Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset, Future Gener. Comput. Syst. 100 (2019) 779–796.
[10] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: an ensemble of autoencoders for online network intrusion detection," arXiv preprint arXiv:1802.09089, 2018.
[11] X. Yuan, C. Li, X. Li, Deep Defense: identifying ddos attack via deep learning, in: IEEE International Conference on Smart Computing (SMARTCOMP), 2017, pp. 1–8.
[12] Yair Meidan, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher, Yuval Elovici, N-baiot—network-based detection of iot botnet attacks using deep autoencoders, IEEE Pervasive Comput. 17 (3) (2018) 12–22.
[13] M. K. Putchala, "Deep learning approach for intrusion detection system (ids) in the internet of things (iot) network using gated recurrent neural networks (gru)," 2017.
[14] Mohamed Amine Ferrag, Leandros Maglaras, Deepcoin: a novel deep learning and blockchain-based energy exchange framework for smart grids, IEEE Trans. Eng. Manage. 67 (4) (2020) 1285–1297.
[15] Y. Meidan, M. Bohadana, A. Shabtai, M. Ochoa, N. O. Tippenhauer, J. D. Guarnizo, and Y. Elovici, "Detection of unauthorized iot devices using machine learning techniques," arXiv preprint arXiv:1709.04647, 2017.
[16] N. Koroniotis, N. Moustafa, E. Sitnikova, J. Slay, Towards developing network forensic mechanism for botnet activities in the iot based on machine learning techniques, in: International Conference on Mobile Networks and Management, 2017, pp. 30–44.
[17] Y.N. Soe, Y. Feng, P.I. Santosa, R. Hartanto, K. Sakurai, Rule generation for signature based detection systems of cyber attacks in iot environments, Bull. Networking, Comput., Syst. and Software 8 (2) (2019) 93–97.
[18] V.H. Bezerra, V.G.T. da Costa, S.B. Junior, R.S. Miani, B.B. Zarpelao, One-class classification to detect botnets in iot devices, in: Anais do XVIII Simpósio Brasileiro em Segurance da Informac¸ ~ao e de Sistemas Computacionais, 2018, pp. 43–56.
[19] E. Hodo, X. Bellekens, A. Hamilton, P.-L. Dubouilh, E. Iorkyase, C. Tachtatzis, R. Atkinson, Threat analysis of iot networks using artificial neural network intrusion detection system, in: International Symposium on Networks, Computers and Communications (ISNCC), 2016, pp. 1–6.

Further reading

[2] T. Bodström and T. Häm aläinen, "State of the art literature review on network anomaly detection with deep learning", Internet of Things, Smart Spaces, and Next Generation Networks and Systems 2018 64 76.
[3] I. Arnaldo, A. Cuesta-Infante, A. Arun, M. Lam, C. Bassias, K. Veeramachaneni, Learning representations for log data in cybersecurity, in: International Conference on Cyber Security Cryptography and Machine Learning, 2017, pp. 250–268.
[4] M. Du, F. Li, G. Zheng, V. Srikumar, Deeplog: anomaly detection and diagnosis from system logs through deep learning, in: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 1285–1298.
[5] B. J. Radford, B. D. Richardson, and S. E. Davis, "Sequence aggregation rules for anomaly detection in computer network traffic," arXiv preprint arXiv:1805.03735, 2018.
[7] Matija Stevanovic, Jens Myrup Pedersen, Detecting bots using multi-level traffic analysis, IJCSA 1 (1) (2016) 182–209.
[8] H. Sedjelmaci, S.M. Senouci, M. Al-Bahri, A lightweight anomaly detection technique for low-resource iot devices: a game-theoretic methodology, in: IEEE International Conference on Communications (ICC), 2016, pp. 1–6.