e-ISSN 2320 –7876 www.ijfans.org
Vol.11, Iss. 12,Dec 2022
 UGC CARE Listed (Group -I) Journal

META CLASSIFIER STUDY THE PERFORMANCE OF IoT-BASED INTRUSION DETECTER

Anirudh Kumar Tiwari[1] Bhavana Narain[2]

[1,2]MATS School of IT, MATS University, Raipur, Chhattisgarh, India

Email ID: {tiwarianirudh646, narainbhawna}@gmail.com

Abstract

The Internet of Things (IoT) is the new paradigm of our times, where digital devices and sensors from across the globe are interconnected with distributed applications and services that impact every area of human activity. With its huge economic impact and its pervasive influence over our lives, IoT is an attractive target for criminals, and cyber security becomes a top priority for the IoT ecosystem. Deep learning may provide a cutting-edge solution for IoT intrusion detection with its data-driven, anomaly-based approach and ability to detect emerging, unknown attacks.

With the increase in the number of internets connected devices, security, and privacy concerns are the major obstacles impeding the widespread adoption of the Internet of Things (IoT). Securing IoT has become a huge area of concern for all, including consumers, organizations as well as the government. While attacks on any system cannot be fully prevented forever, real-time detection of the attacks are critical to defending the system in an effective manner. Limited research exists on ancient intrusion detection systems suitable for IoT environments. This detection platform provides security as a service and facilitates interoperability between

various network communications protocols used in IoT.

This whole matter will directly connect the police with the crime location which eases the police can reach that location. GPS will be used for location detection. In our work, we have collected datasets with the help of a digital camera that is attached to an IoT device. In the first part of our paper, we have discussed the ground so four works under the introduction of crime, digital image processing, GPS, and IoT. In the second part of our

work, we have discussed the methodology of our work here sensor board, and GPS setting has been discussed along with the dataset. There are several data collection technologies in the IoT. The most used technology is the Warless sensor network (WSN) uses multi-hopping and self-organization to maintain control over the communication network nodes.

1. Introduction

The emergence and development of new technologies such as sensors, broadband 5G and beyond wireless communications, radio frequency identification, smartphones, portable computers, industrial automation, semi-autonomous vehicles, satellites, cloud computer, and others, converge into what we broadly refer to as the Internet of Things (IoT), an all-encompassing network where smart devices and computational units are inter-connected, communicating and interacting with each other. At the same time, cyber-physical systems, comprising IoT devices, control critical infrastructures. IoT ecosystems, and as a consequence, new forms of cyber-attacks merge that either use IoT devices as a stepping stone towards other systems or target IoT devices themselves.Network Intrusion Detection system (NIDS) can define the embedded process in networking for devices like smart sensor-inspired devices & under a service-oriented architecture (SOA) to regulate independently as an anomaly-based NIDS or integrated, transparently, during a very distributed Intrusion Detection System (DIDS) [4]. A ramification of intrusion detection approaches is present to resolve this severe issue but the foremost problem is performance. It is vital to increase detection rates and reduce warning rates within the world of intrusion detection. So to detect the intrusion, various approaches are developed [6]. An Intrusion Detection System (IDS) can discover malicious activities and irregularities within the network and provide a fully important basis for network defence. Thanks to the event of cloud computing, social networks, additionally as mobile cloud computing, IDS has become even more important than before ([7][8]). Network Intrusion Detection System (IDS) tries and identify unauthorized, illicit, and anomalous behaviour based solely on network traffic to support deciding network preventive actions by network administrators [10]. Many researcher share contributing to this field for the last twenty years. During this paper, certain literature survey has been done to display some past research work.

Cyber security attacks are becoming one of the most serious threats to IoT security. These attacks occur in various forms, targeting different resources on a variety of IoT devices. These attacks tend to compromise one or more device(s) in an IoT network which can be further utilized as a "resource" or "platform" for attacks such as distributed denial-of-service, and fraudulent activities such as ransomware, opportunistic-service stealing, and information ex-filtration. Hence important for safeguarding such data.

2. Methodology Dataset and Tools

2.1 Classification Algorithm for IoT

Classification Algorithms can be further divided into the Mainly two categories:

- **Linear Models**
  - Logistic Regression
  - Support Vector Machines
- **Non-linear Models**
  - K-Nearest Neighbours
  - Kernel SVM
  - Naïve Bayes
  - Decision Tree Classification
  - Random Forest Classification

2.2 Classification Algorithm for IDS

Classification approach	Techniques
1) Decision Tree	A decision tree is a type of supervised machine learning used to categorize or make predictions based on how a previous set of questions were answered. A model is a form of supervised learning, meaning that the model is trained and tested on a data set containing the desired categorization.
2) Bayesian Network	A Bayesian network is a compact, flexible, and interpretable representation of a joint probability distribution. It is also a

	useful tool in knowledge discovery as directed acyclic graphs allow the representation of causal relations between variables.
3)K-Nearest Neighbour	The k-nearest neighbour's algorithm, also known as KNN or k-NN, is a non-parametric, supervised learning classifier, which uses proximity to make classifications or predictions about the grouping of an individual data point.
3) SVM	In machine learning, support vector machines (SVMs, also support vector networks) are supervised learning models with associated learning algorithms that analyze data for classification and regression analysis.

3. META Classifier for IoT-based Intrusion Detection

Meta-learning in machine learning refers to learning algorithms that learn from other learning algorithms.
Most commonly, this means the use of machine learning algorithms that learn how to best combine the predictions from other machine learning algorithms in the field of ensemble learning.

Nevertheless, meta-learning might also refer to the manual process of model selecting and algorithm tuning performed by a practitioner on a machine learning project that modern autonomous algorithms seek to automate. It also refers to learning across multiple related predictive modelling tasks, called multi-task learning, where meta-learning algorithms learn how to learn.

It even refers to multi-task learning which involves learning across several related predictive modelling tasks. Here, meta-learning algorithms can learn how to learn. Meta-learning algorithms make their own predictions by using the output or predictions of existing machine-learning algorithms as input and then predicting a number or class label. You could say that meta-learning occurs one level above machine learning. Machine learning learns the best way to use the information found in data to make predictions, while meta-learning learns the best way to use the predictions that machine learning algorithms have made to make predictions. A meta-learning algorithm or a meta-learning machine

learning algorithm can be simply referred to as a meta-algorithm or a meta-learner in short-hand. Meta-learning can be used to observe the performance of several machine learning models about learning tasks, learn from metadata, and speed up the learning process for new tasks.32.1 What techniques are used in meta-learning?

Here are some of the approaches that are used in meta-learning.

3.2 Metric Learning

This refers to learning a metric space for predictions. It delivers good results in few-shot classification tasks. The main idea in metric learning is very similar to nearest neighbors algorithms (k-Nearest Neighbours classifier and k-means clustering).

3.3 Model-Agnostic Meta-Learning (MAML)

In MAML, the neural network is trained with the use of examples to adapt the model to new tasks at a quicker pace. It is a general optimization and task-agnostic algorithm which is employed for the purpose of training the parameters of a model for quick learning with a small number of gradient updates.

3.4 Recurrent Neural Networks (RNNs)

Recurrent neural networks are a type of artificial intelligence. These RNNs are applied to several machine-learning problems. They are especially used on problems that have sequential data or time-series data. They are generally used for language translation, speech recognition, and handwriting recognition tasks. In meta-learning, an RNN is used as an alternative to creating a recurrent model that has the ability to gather data sequentially from datasets and process this data as new inputs.

3.5 Stacking or Stacked Generalization

Stacking is a sub-field of ensemble learning and is used in meta-learning models. Supervised as well as unsupervised learning gain advantages from stacking. Here is the process involved in stacking:

- Training learning algorithms using the data that is available.
- Creating a combiner algorithm to combine the predictions of the learning algorithms (known as ensemble members).
- Make use of the combiner algorithm for the purpose of making the final predictions.

3.6 Convolutional Siamese Neural Network

A convolutional Siamese neural network comprises two twin networks. Their outputs are trained jointly on top using a function to understand the relationship between pairs of input data samples.

The twin networks share the same weights and network parameters. They refer to the same embedding network that learns an efficient embedding to reveal the relationship between the pairs of data points.

3.7 Matching networks

Matching networks learn a classifier for any small support set. The classifier defines a probability distribution over output labels with a specific test example. It essentially maps a small labeled support set and an unlabelled example to its label, eliminating the need to fine-tune for adapting to new class types.

3.8 LSTM Meta-Learner

An LSTM meta-learning algorithm finds the exact optimization algorithm that is employed for training another learner neural network classifier in the few-shot regime. The parametrization makes it possible for it to learn appropriate parameter updates specifically for the scenario where a set number of updates will be made. It even learns a general initialization of the learner network that enables the quick convergence of training.

4. Bagging Algorithm for IoT-based intrusion detection

Bagging, also known as Bootstrap aggregating, is an ensemble learning technique that helps to improve the performance and accuracy of machine learning algorithms. It is used to deal with bias-variance trade-offs and reduces the variance of a prediction model. Bagging avoids overfitting data and is used for regression and classification models, specifically for decision tree algorithms.

4.1 Steps to Perform Bagging Algorithm

- Consider there are n observations and m features in the training set. You need to select a random sample from the training dataset without a replacement
- A subset of m features is chosen randomly to create a model using sample observations
- The feature offering the best split out of the lot is used to split the nodes
- The tr
- ee is grown, so you have the best root nodes
- The above steps are repeated n times. It aggregates the output of individual decision trees to give the best prediction

5. Result and Discussions

In this paper, we have taken four statistical readings of thousand user IDs. This used id was generated by an IoT device. The ioT device was placed in the police station of Tikrapara Raipur. The minimum value of the image was 18 of used id 101. The maximum value is 33. The mean value is 27.5 and the standard deviation is 5.318. The latitude and Longitude of the image taken are also calculated in Meta Classifier.

Table 1: Statistical Result of META Classifier

Classifier Method	Attribute	Min	Max	Mean	Std Dev
META	**UserId(101)**	18	33	27.5	5.318
	Latitude	21.23	22.72	21.97	0.79
	Longitude	75.85	81.64	78.73	3.08

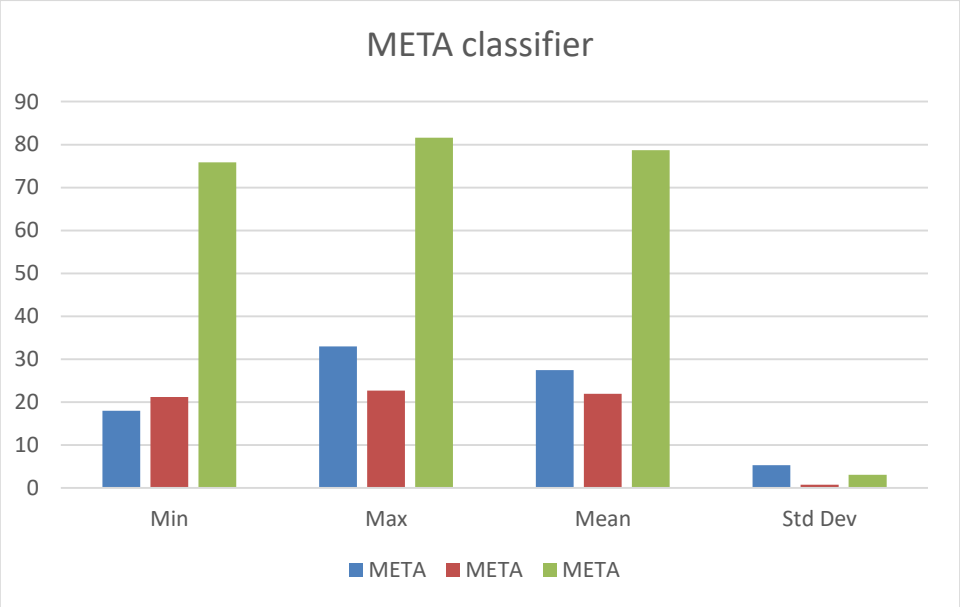

Fig. 1 Statistical Result of User id 101

Table 2: Statistical Result of Bagging Classifier

Bagging Algorithm	Correlation Coefficient	Root Mean Squared Error	Relative Absolute Error	Root Relative Squared Error	Total Number Of Instances	Mean Absolute Error
	0.91	3.34	3.34	5.0054	4.38	3.03
	0.91	3.92	3.92	5.6	4.42	3.074
	-0.62	76.53%	76.53%	100.10%	113.44%	75.83%
	0	78.84%	78.84%	98.54%	109.56%	76.23%
	0	8	8	8	3	2

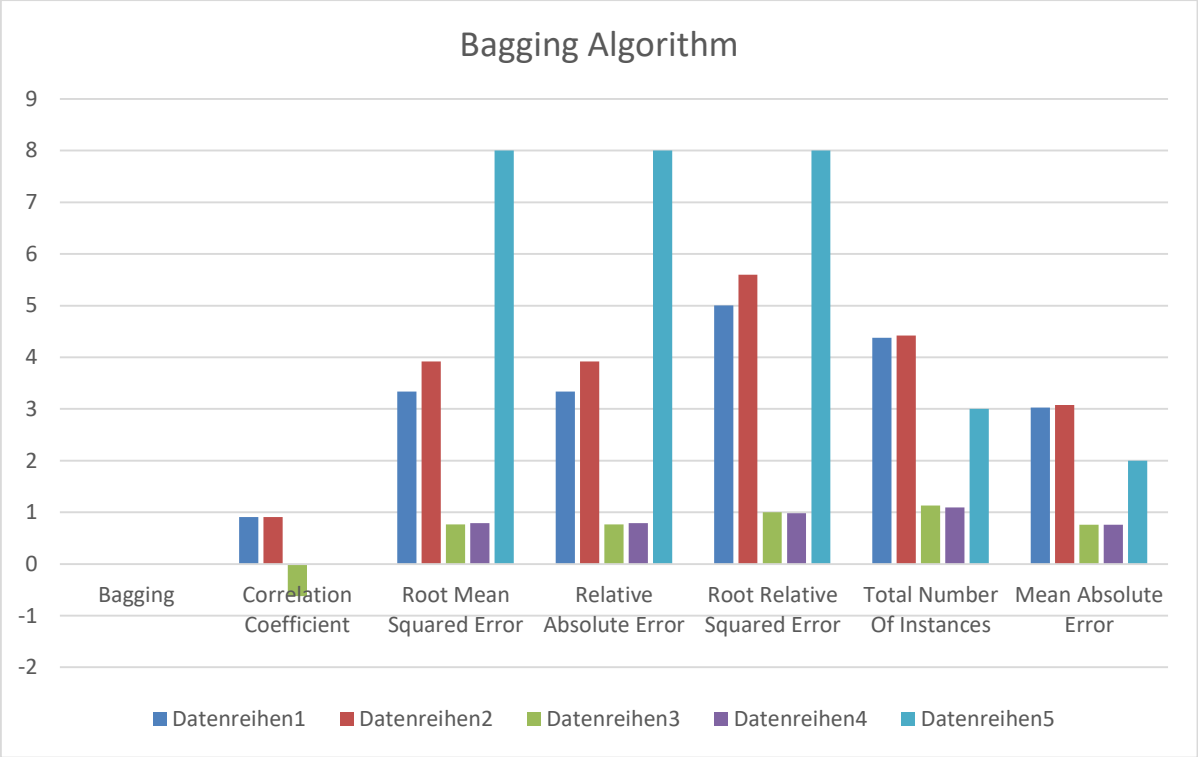

Fig. 2 Statistical Result of Bagging Algorithm

5.1. Mean absolute error

In the context of machine learning, absolute error refers to the magnitude of difference between the prediction of an observation and the true value of that observation. MAE takes the average of absolute errors for a group of predictions and observations as a measurement of the magnitude of errors for the entire group. Root mean squared error. Root mean squared error (RMSE) is the square root of the mean of the square of all of the errors. The use of RMSE is very common, and it is considered an excellent general-purpose error metric for numerical predictions. Relative Absolute Error

Relative Absolute Error (RAE) is a way to measure the performance of a predictive model. It's primarily used in machine learning, data mining, and operations management. RAE is not to be confused with relative error, which is a general measure of precision or accuracy for instruments like clocks, rulers, or scales.

5.2. The Root Relative Squared Error

The Root Relative Squared Error (RRSE) is defined as the square root of the sum of squared errors of a predictive model normalized by the sum of squared errors of a simple model. In other words, the square root of the Relative Squared Error (RSE).

6. Conclusion & Future Work

In this paper, we have presented a literature survey on network intrusion detection systems. Network security is playing a vital role in altogether styles of networks. Intrusion detection has attracted considerably more interest from researchers and industries so currently it's a sensible choice for networking users for security purposes. After some years of research, the community still faces the matter of building reliable and efficient NIDS, which are capable of handling large amounts of knowledge, with aging patterns in real-time situations. The scope of the work on classifying intrusion detection systems, reviewing the various methods of detecting an anomaly, performance of those methods was supported by past and up to now works revealing the benefits and drawbacks of every one of them.

References

[1] Stefanos Tsimenidis, Thomas Lagkas, Konstantinos Rantos, "Deep Learning in IoT Intrusion Detection", Journal of Network and Systems Management (2022) 30:8, https://doi.org/10.1007/s10922-021-09621-9.

[2] Shiven Chawla, "Deep Learning based Intrusion Detection System for Internet of", 2017.

[3] Francisco Macia-Perez, Francisco J. Mora-Gimeno, Diego Marcos-Jorquera," Network Intrusion Detection System Embedded on a Smart Sensor", IEEE, 2010.

[4] Santosh Kumar Sahu, Sauravranjan Sarangi, Sanjaya Kumar Jena," A Detail Analysis on Intrusion Detection Dataset", IEEE, © 2014, 978-1-4799-2572-8/14.

[5] SravanKumar Jonna lagadda, Ravi Prakash Reddy, "A Literature Survey and Comprehensive Study of Intrusion Detection," International Journal of Computer Applications, November 2013, 0975–8887, Vol.81, No.16.

[6] Kai Peng, Victor C .M. Leung,and Qingjia Huang, "Clustering Approach Based on Mini Batch K means for Intrusion Detection System Over BigData", Special Section on Cyber-Physical-Social computing and Networking, February 28, 2018, Digital Object Identifier 10.1109/ACCESS.2018.2810267,Vol.6,2169-3536,2018IEEE.

[7] R. Vinayakumar, MamounAlazab, K. P. Soman, Prabaharan Poornachandran, Ameer Al- Nemrat, and Sitalakshmi Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System", IEEE Access, April11, 2019, 10.1109/ACCESS.2019.2895334. Vol.7,2169-3536, 2019IEEE.

[8] Longzhi Yang, Jie Li, Gerhard Fehringer, Phoebe Barraclough, Graham Sexton, Yi Cao, "Intrusion Detection System by Fuzzy Interpolation",2017 IEEE international conference on fuzzy systems (FUZZ-IEEE),2017, pp.1-6.

[9] Biswanath Mukharjee, L. Todd Heberlein and Karl N. Levitt, "Network Intrusion Detection", IEEENetwork,May/June1994,0890-8044/94/$0.4.00,©1994.

[10] Clive Grace, "Understanding Intrusion Detection Systems", PC Network Advisor, www.itp- journals.com, September2000, Issue122, pp.11.

[11] Ahmed Awad E. Ahmed and Issa Traore, "Anomaly Intrusion Detection based on Biometrics", 2005 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY, June2005, ISBN555555555, ©2005IEEE.

[12] Robert Mitchelland Ing- Ray Chen, "A Survey of Intrusion Detection Techniques for Cyber- Physical Systems", ACM Computing Surveys, March2014, Vol.46, No.4.

[13] Nasrin Sultana, Naveen Chilamkurti, Wei Peng, Rabei Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches", Peer-to-Peer Networking and Applications, https://doi.org/10.1007/s12083-017-0630-0,12January2018.

[14] Christos Xenakis, Christoforos Panos, Ioannis Stavrakakis, "A Comparative Evaluation of Intrusion Detection Architectures for Mobile AdHoc Networks", computer & security 30 (1),63-80,2011.

[15] Abdelouahid Derhab, Abdelghani Bouras, Mustapha Reda Senouci, and Muhammad Imran, "Fortifying Intrusion Detection System in Dynamic AdHoc and Wireless Sensor Networks", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, December 2014, ArticleID608162, pp.15,http://dx.doi.org/10.1155/2014/608162.

[16] Quamar Niyaz, Weiqing Sun, Ahmad YJavaid, and Mansoor Alam, "A Deep Learning Approach for Network Intrusion Detection System", BICT2015, December03-05, New York City, United States, Copyright©2016ICST, DOI10.4108/eai.3-12-2015.2262516.

[17] Chirag N.Modia, Dhiren R.Patela, AviPatelb, Muttukrishnan Rajarajanb, "Integrating Signature Aprioribased Network Intrusion Detection System (NIDS) in Cloud Computing", 2nd International Conference on Communication, Computing & Security (ICCCS-2012),6,2012,905–912.

[18] Hu Zhengbing, Li Zhitang, WuJunqi, "A Novel Network Intrusion Detection System (NIDS) Based on Signatures Search of Data Mining", e-Forensics2008, January21-23,2008, Adelaide, Australia, ©2008ICST978-963-9799-19-6.

[19] Jihyun Kim, Jaehyun Kim, Huong Le Thi Thu, and Howon Kim, "Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection", International Conference on Platform Technology and Service, Deccember31, 2015.

[20] V.Jyothsna, V. V. Rama Prasad, "A Review of Anomaly based Intrusion Detection Systems", International Journal of Computer Applications, September 2011, 0975–8887, Vol.28, No.7.

[21] Abhishek Das, David Nguyen, Joseph Zambreno, Gokhan Memik, and Alok Choudhary, "An FPGA-Based Network Intrusion Detection Architecture", IEEE Transactions on Information Forensics and Security, March2008, Vol.3, NO.1.

[22] Chuanlong Yin, Yuefei Zhu, JinlongFei, Xinzheng He,"A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks", IEEE Access, 2169-3536,2017IEEE,Vol.5,2017.

[23] Hung-Jen Liao, Chun-Hung Richard Lin, Ying- Chih Lin, Kuang-Yuan Tung," Intrusion detections system A comprehensive review", Journal of Network and Computer Applications 36, Accepted11, September2012, Available online23, September2012,16–24.

[24] Mehdi Hosseinzadeh Aghdam, and Peyman Kabiri, "Feature Selection for Intrusion Detection System Using Ant Colony Optimization", International Journal of Network Security, May2016, Vol.18, No.3, PP.420-432.

[25] Wei Lu and IssaTraore, "Detecting New Forms of Network Intrusion using Genetic Programming", Computational Intelligence, 2004, Vol.20, No. 3.