Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 9, No. 2, May 2021, pp.873-884

Detecting insider threat within institutions using CERT dataset and different ML techniques

Mohammed Dosh
Computer Science Department, College of Education for Girls, University of Kufa, Iraq

ABSTRACT

The reason of countries development in industrial and commercial enterprises fields in those countries. The security of a particular country depends on its security institutions, the confidentiality of its employees, their information, the target's information, and information about the forensic evidence for those targets. One of the most important and critical problems in such institutions is the problem of discovering an insider threat that causes loss, damage, or theft the information to hostile or competing parties. This threat is represented by a person who represents one of the employees of the institution, the goal of that person is to steal information or destroy it for the benefit of another institution's desires. The difficulty in detecting this type of threat is due to the difficulty of analyzing the behavior of people within the organization according to their physiological characteristics. In this research, CERT dataset that produced by the University of Carnegie Mellon University has been used in this investigation to detect insider threat. The dataset has been preprocessed. Five effective features were selected to apply three ML techniques Random Forest, Naïve Bayes, and 1 Nearest Neighbor. The results obtained and listed sequentially as 89.75917519%, 91.96650826%, and 94.68205476% with an error rate of 10.24082481%, 8.03349174%, and 5.317945236%.

Keywords: Insider threat, CERT dataset, Cybersecurity, Attacker's psychology, IT sabotage

Corresponding Author:

Mohammed Dosh,
Computer Science Department
College of Education for Girls
University of Kufa, Iraq
E-mail: mohammedh.dosh@uokufa.edu.iq

1. Introduction

Insider attackers represent a malicious activity performed by an authorized person inside the organization. It is one of the most prevalent and dangerous situations in various threats in security issues that are faced by companies, organizations, and institutions. Among all types of attacks, the insiders have the highest level of cost and hard of detection because the insiders have the required knowledge, authority, organization network structure, and security procedures to access all the institution network information [1]. The survey of cybersecurity verified that 53% of institutions and 42% of United States federal agents suffering from insider attacks yearly [2]. The organization insider attacks have the percent of 25% of all the threats this percent increasing gradually [3]. A part of insider threats tends to report cases of combustion incidents, including burnt data, customer records, trading secrets, theft of personal identification information, and destruction of IT systems [4]. Network-connected systems are an essential and sensitive part of any company where data associated with employees and clients and their confidence are stored to be processed, Therefore, the insider threat is a major threat against cybersecurity, which must be addressed with the main priorities to assure the continued safety of these systems and hence the functions of the institution. The threat definition was mentioned in a technical report issued by CERT Insider Threat. It has been defined as threats implemented by malicious or non-intentional persons whose permission to enter the institution’s network, systems, and data are used negatively to affect the confidentiality of this data. Malicious activity relevant to insider intimidation can be carried out deliberately by spiteful insiders such as sabotaging information systems and revealing confidential information, as well as by an unintentional insider, such as neglecting the use of authorized resources [4]. Apart

from the traditional tasks for intrusion detection, there are various challenges related to the detection of internal threats, because the informed person has the authorization to enter all the network sites belong to the organization, sub systems and possesses sufficient information about the institution layers security, in addition to that the art of insiders with malicious intent in most institutions their activities are irregular. Consequently, data available to describe their activity and movement are not well documented and are scarce [5].

The challenges of insider threat detection may originate from process requirements and data kind's wide range investigation in institutional conditions, network traffic, accessing web logs, and files to history of email or employee information. The data also greatly fluctuates prepared by the corporation. Consequently, only a diminutive portion of the institutions have the tools and human resources for describing user behavior and purpose from the data collection monitoring.

This paper has been performed an evaluation process for ML application routines in understanding enterprise network systems and malicious inside institutions. The model has been proposed and evaluated workflows for detecting user-focused internal threats, from collecting pre-processing data to analyzing data with ML techniques, reports information and analyzing. The designed methodology intends for helping the analysts of cybersecurity to learn from only a diminutive fraction of common employee actions and identify malicious insider liveliness to distinguish threats under anonymous data and produce valuable penetrations [3].

The research intends to obtain the following contributions: (1) realistic requirement has been hypothesized for training ML procedures for producing outcomes that simulate the real environments of the world, highlighting comparative differences to training corresponding to various conditions; (2) data processing technologies have been exploring to affects the obtaining of multi-levels of data accuracy with informative detail for analyzing data [3]. (3) comprehensive results reporting process has been provided with different ML techniques, and malicious cases are inspected, to have a preferable insight of performance.

The other section of the paper is constructed as the following. The second section behavioral and definitional issues. The third section presents the background and related work. The fourth section presents the proposed methodology with the dataset, data preprocessing steps, feature extraction, normalization, the ML algorithms used, results, and evaluation metrics. Section 5 conclusions and suggested future works.

2. Behavioral and Definitional Issues

The requirement of search should be clearly described structures. [6] [7] Once the validity proofs are defined, they are bounded to the context of the research in which they are presented. [8] For instance, a method with characterizing insider threats arises from whereby people and establishments describe an "insider", that is, an association member. Public-private partnerships moreover, blur the boundaries that separate insiders from the outsiders [9] producing separate analytical problematical divisions. Therefore, how IT operates in an obtained critical investigation to determining its relevance and generality.

Insider Threat Descriptions. Representations of an insider threat fluctuate extensively [10], [11]. All too often, the theory is left indeterminate or indeterminate, with studies indicating non-adaptive organizational behavior with little modification. For instance, “Insider threat indicates harmful acts that trusted insiders may commit”, [12], “A malicious insider appears when a trusted user of the information system behaves in a way that the security policy behaves is defined as unacceptable. ". Likewise, the omission to report questionable behavior was described as a "passive" insider threat. [13] Broad interpretations are crucial concerns for valid credentials and prognostication so that all employees should be identified as insider threats.

Intentional explanations were judged, highlighting considerations [14] or malice. Additional definitions also involve intentional behavior that is not malicious [15, 16] or that does not immediately address intention. [17] concerning these descriptions, insider threats imitate behaviors that contrast with methods, procedures, and priorities that the institution has deliberately or accidentally set. Examples of insider threats entail destroying/deleting important knowledge assets, performing unauthorized data modification or records, copying under unauthorized conditions, data or records extraction, intended or accidental interruption of networks, destruction of facilities, eavesdropping, and beams sniff. From aforementioned attitude, models remain succinct significant than the actuality that they diverge from acceptable norms [18].

Researchers should additionally attempt to provide a basic characteristic among types of insider threats according to the data from employee profiles. [19] as Salem et al. [20] Representation, there are three general kinds of methods: host-based user profiling (web and operating systems), sensor-based for networking (user behavior on the network), and integrated procedures that join among the characteristics of the sensor and user profiling. Utilizing a particular method depends on the kinds of insider threat discovery. Furthermore, that will change from unintended insider threats that could hold the consequence of social engineering struggles [21, 22].

A case-based method has been applied by Band et al. requirement represent the analytical portions of 3 by behavior variations [23] However, the insider behavior implications conflicts whether it reproduces disguises or changes. [20] Disguisers are supposed the identification the authorization of the network employee. [24, 20, 25] Considering that employees work in a comparatively uniform manner, disguises are discovered by discerning differences in user action that do not match an actual profile. Instead, failures are considered authorized employees who serve with relevant cohesion within the network. authorized people longing to enter the same locations of file forming disclosure also more complex. Crucially, the leak does appear for transpiring outside the network.

While sometimes referred to as "intentions," are limited detail about these purposes or how they have different behavior. A discovering of the attacker's psychology further lacked [26]. Anderson and Pearson [34] observe in their brutality account the nature of “deviant” behavior in the workplace disregards personal impulses and the communicative circumstances required to perfectly predict behavior within an association. Many insider threat patterns fail to recognize this feasibility or identify key social dimensions [26],[27] Using transcripts, Searle and Rice [28] combined characters of impulse into their insider threat organization. Back of previous interviews correlated to three significant circumstances within the institution, they recognized four distinct types of insiders.

Insiders that disappointed to control their behavior inadvertently violated the rules (the omissions), and regularly engaged in abnormal behavior that might indicate a sedate violation of workplace criteria and systematic commitment in the grave and secondary violations in the workplace Standards have joined in little correlative aggressive (retaliatory) or negative (retraction) behaviors focused towards individuals or the institution (avengers). Furthermore, they also conceive of individuals who have disappointed to report suspicious behavior. While introducing informational divisions, their investigations do not regularly link those divisions to basic psychological dimensions such as impulse.

3. Related works

Detecting insider threats is a hard research problem, not only for the research inhabitants but also for the country's organizations and agencies, and cybersecurity companies. The US National Insider Threat Task Force and CERT Insider Threat Center should be declared collective supervision for helping prevent and alleviate insider threats in managerial situations. [29] [30].

The reference of the research describes 20 practices institutions should achieve crosswise the corporation to avert and discover insider threats, addition to case examinations of companies have slipped for detecting insiders [29].

Liu et al. Provided an overview of the research literature on insider threats, and associated cybersecurity concerns, including malware and superior tenacious threats [31] moreover Homoliak et al. Introduced a taxonomy structure and insider threats novelty categorization [32].

Since the problem of the threat accociated with human factors, several researches techniques solving the difficulty by applying psychological patterns and principles of making the decision [33] [34] [35].

Padayachee implemented contingency criminology hypotheses to imagine insider threats, as well as speculation measures of minimization for helping to relieve insider threats [33].

Greitzer et al. Suggested a framework for the model prediction that use many data sources integration and psychological/motivational determinants to assist the analyst in discovering essential danger behavior, implemented approaches of criminology opportunity to visualize insider threats, and limitation of opportunity measures to help mitigate insider threats [34].

Legg et al. suggested a structure for insider threats modeling depends on observations of psychological and behavioral aspects. The structure supports the analyst for clarifying and represent possible insider threats of multiple domains, such as the policies of organizations and behavior of the human. [35].

A huge quantity of data has been given and gained by any organization every day. Solution based on ML are between the multiple promising techniques to solving challenges of cybersecurity of the current era [36].

The benefit of ML is the capability of automatically learning from a massive quantity of data and distinguish patterns that have the most similar characterize malicious motions or anomalous behaviors [37].

They further recognized any malicious user notices within the guide research that could notify this design from an insider threat detection system [38].

An aberration discovery represents a common method that uses ML techniques for detecting insider threats, in which models of typical employee performance are created and abnormality has been described as aberrations

of natural behavior. the abnormality signaling, this situation, refers to innovations in the behavior of the user as a potential first sign of insider threats. Parveen et al. have proposed graph-based model with educational assumption guidance method to discovering insider threats according data flow. To do this, quantitative pattern dictionaries are generated for each piece of data and the the consideration of data has been referred to as abnormality if it including a high distance dictionary usual patterns [39].
An additional method for detecting anomalies has been modeled to employ series of human activities for abnormal sequence detection.
Rashid et al. proposed a system with a Hidden Markov model to acquire weekly the series of normal activities for each user from the common activities. series of abnormality activity detected by the model refers to the insider threats [40].
Many insider threat discovery systems have been supported by the DARPA (Defense Advanced Research Projects Agency) ADAMS (Anomaly Detection at Multiple Scales) project. The project purpose is "identify patterns and anomalies in very large data sets" for preventing and detecting insider threats [41] [42] [43].
Various algorithms were used to detect anomalies, including hidden Markov models and Gaussian mix models, in a group on user activity log data to identify insider threat indicators [44].
Eldardery et al. Used anomaly detectors combined in hybrid form for user activity logs in several different discover data of double classes of insiders - the intrusive insiders from the blending, and insiders who had an abnormal action in behaviors [41].
Disguise detection policies are suggested based on the discovery of anomalies in user search and the behaviors of accessing file [45] [46].
Javai et al. I applied various machine learning methods to data that have organized to detect abnormality and initial indications of "withdrawal", as both may indicate internal threats [41].
The capabilities of various ML technologies, such that the Bayesian-based approaches [48][49], decision tree [47], and the self-organizing map [50] also have been tested to discover insider threats. real-time learning methods have used to distinguish the conditions for unusual user behaviors.
Tor et al. Suggested an approach for discovering abnormality using the enterprise of deep neural network, or a model per user neural networks have been used for builds scores for abnormality [51].
Bose et al. Propose a model that uses moderated and unsupervised extendibility learning techniques to integrate a stream of heterogeneous data to recognize abnormalities and insider threats [52].
On other side, Le et al. Conventional algorithms of genetic programming supporting two behavioral theories: static and dynamic, to check the evolutionary probability computation in detecting the insider threat [53].
In this paper different ML techniques have been applied to the CERT dataset after preprocessing and feature extraction for detecting insider threat, and the performance of these technique have been compared.

4. Methodology

4.1. Dataset

Insider threat recognition, many suitable data sets are not available. Therefore, the insider threat data set published by CERT (Carnegie Mellon University) has been applied in this research [54]. "R4.1 and R4.2" dataset has been used for the analysis. This dataset contains six kinds of data logs: HTTP, login, email, psychometry, device, and file. All activities of 1000 employees over 17 months are contained in this dataset [55].

4.2. Preprocessing

Pre-processing is significant for identifying insider threats appropriately but likewise for cybersecurity duties in general. the best monitoring method coupled with suitable data accumulation allows the successful employment of machine learning procedures and assists security analysts in producing the right decisions. The data collected from the environments of the institutions for that the data sources are wide and variable. The variety of resources construct data with different patterns. [29] [56] in this paper the data have been organized into two main categories: the first category contains the activity log data .It represents the real-time sources of the data that require to accumulate and be prepared in a suitable time. form in order of speedy detection and response to malicious and anomalies. This category came from different system logon such as file accesses, firewall logs, emails, and capturing network traffic, and web. The second category contains the structure of organization and user information including employee information, relationship with other employees, and the

employee role in the institution. The second category of data acts as the context data or the background this category has the more complex data including behavioral model and psychometric of users. Assisting to manipulate data and create features, user context models are obtained for all users in the institution. The forms include the auxiliary information associated with every user, such as restricted devices, relations with other employees, tasks, hours of work, authorized access, etc. depend on user context models, feature vectors have been created that summarize user activity immediately and regularly from the input data.

4.3. Features extraction

Features extraction can be performed using input data and user context to obtain user data vectors that are used for training ML models. At first, data aggregated from different resources depending on used ID according to aggregation conditions C such as the performed task numbers and time duration. The second generates the numeric vector X_c also called data instances by applying features extraction on the aggregated data. The numeric vector with fixed length N summarized users' actions and includes the information of the user. Data categories have been encoded to numerical form to apply ML techniques. The features have been provided are frequent features that represent the number of different types of actions performed by the user during the proceeding of the aggregation process such that date, user, PC, activity, and vector.

4.4. Normalization

The status of the raw data is not ordinarily proper for processing by data mining and machine learning techniques. Data normalization is a method of molding raw data values to different forms with characteristics of more useful for modeling and analysis. It is necessary to prevent the difference of huge values that is controlled the results. So, the term normalization can be applied for producing a normal feature. Normalization aspires to guarantee that a whole set of values have a special characteristic. So that all the features should be revealed at the equivalent unit of determination. There're various techniques of normalization specifically Min-Max Normalization, Z-Score Normalization, and Decimal Scaling Normalization [57]. Min-Max normalization method will be addressed because it has been implemented in this paper.

Min-Max normalization arranges a transformation that is linear on the source data. Consider that min(A) and max(A) are the smallest and the biggest values to feature (A). Min-Max Normalization maps the value (V) from (A) into V' at a domain [new_min(A), new_max(A)]. The equation below has been applied for calculating the value [58]:

$$\bar{v} = \frac{v - \min(A)}{\max(A) - \min(A)} (new_{\max(A)} - new_{\min(A)} + new_{\min(A)} \quad (1)$$

Where:

Max(A): is the highest value for the native values for any feature.

Min(A) : is the lowest value for the native values for any feature.

$new_{\min(A)} new_{\min(A)}$ and $new_{\max(A)} new_{\max(A)}$ are the highest and lowest interval for values.

v: represents the value of the feature.

4.5. Classification

4.5.1. Random forest

It refers to its name, includes a great number of unique decision trees that run multiple forms in order of obtaining the better performance of prediction. Each tree included in random forest splutters produces a prediction for a class. This class represents the class that has the most votes to become the prediction model. The random forest visualization obtaining a classification. The fundamental idea of the random forest is manageable however powerful. The knowledge of organizations. In science-speak of data, the random forest model theory to operate in benefit way: A large number of uncorrelated trees run permission will surpass every single-component technique. the key represents the low that associate among the models. Exactly such that low-association characteristics are collected collectively to construct a purse greater than the whole parts, independent techniques can generate aggregate forecasts which have a high accuracy of any individual forecast. The purpose of astonishing effect because the trees preserve each other from their singular error. Some trees may have a high error rate, many other trees will be accurate, so as a collection the trees can influence in the correct direction. So, the requirements for a random forest to operate perfectly are:

- There should obtain some original sign in the build features so models created with those features run

more beneficial than random guesswork.
- The predictions produced by singular trees should beget low associations with each other.

4.5.2. Naïve Bayes

Naive Bayes is a probabilistic classifier its performance depends on Bayes theory. with powerful (naïve) confidence hypotheses between the characteristics. They are between the easiest Bayesian interface models but joined with kernel density estimation, they can obtain greater accuracy levels. The naïve Bayes classification model has highly scalable, expecting several linear parameters in the number of features or predictors problem learning. Maximum-likelihood training should be accomplished by estimating a closed-form formulation, which requires a linear time, rather than the costly iterative estimation used by the various classification methods [58].

4.5.3. Nearest Neighbor

It is one of the ML lazy learner techniques. When the test sample ready to classify the training, a step applies. The proximity between the test state and all the training sets has been calculated using proximity measures. The nearest neighbor has been chosen according to the proximity to the test sample. The class of the test sample should be equivalent to the class of the nearest instance in training. [47]. Euclidian distance, Manhattan Distance, and Minkowski Distance are an example of the proximity measures. The following equation explains the Euclidian distance used in this research [58].

$$Euclidian(x,y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)} \quad (2)$$

x, y = two points in space of *N* states.
n= total number of instances in space.

4.5.4. Evaluation

Performance measurements have scalability and variation in this research two performance measures have been used the Root Mean Square Error (RMSE) and the Mean Absolute Error (MAE)

MSRE is a commonly applied performance measure of the variations between the test set predicted by a classifier and the actual value. The RMSD represents the square root of the second sample moment of the contrasts between estimated values and actual values or the quadratic average of these variations. These errors are called *residuals* when the computations are accomplished across the data unit that is used for predicting and are denominated as *errors* when calculated out-of-sample. The RMSE labors to aggregate the importance of the errors in estimation for multiple data circumstances into a unique measure of estimative power. RMSE is an accuracy measurement, applied to compare forecasting errors of various classification models for a special dataset and not between datasets, as it is scale-dependent.

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i' - y_i)^2} \quad (3)$$

y'i =esmated.
yi = actual.
n= total number of instances.

MAE is a statical performance measure between joined investigations formulating the same phenomenon. suppose of Y versus X contain comparisons of estimated versus actual, consequent time against initial time, and one method of measurement against an alternative method of measurement. MAE is computed using the following formula:

$$MAE = \frac{\sum_{i=1}^{n}|y_i - x_i|}{n} \quad (4)$$

y_i = estimation.
x_i = actual.

n= total number of instances.

5. Results

The results have been obtained by applying three ML algorithms Random Forest, Naive Bayes, and 1Neaerest Neighbor. The results listed as follows:

1- Applying the Random Forest technique have been accomplished with two kinds of training:

With 66% training set and the remaining test set, the result summarized in figure (1) with an accuracy of 89.59040507% and an error rate of 10.40959493%

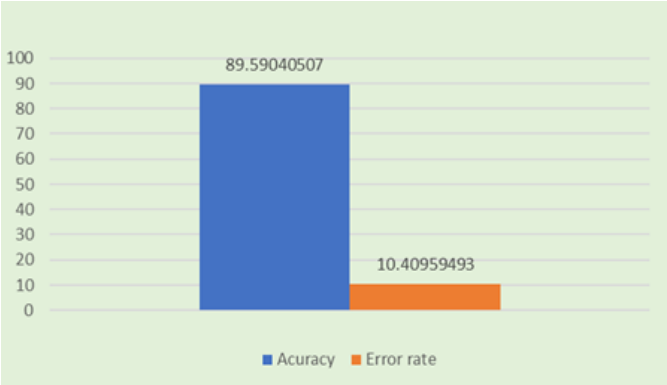

Figure 1. Random Forest with 66% training results

The performance measurement Root Mean Square Error (RMSE) and Mean Absolute Error (MAE) has been summarized in Figure 2.

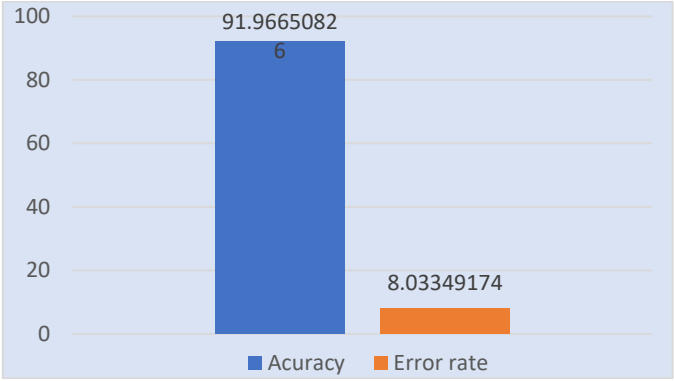

Figure 2. The performance measurements RMSE and MAE for Random Forest with 66% training set.

With the 10-Fold training set, the result is summarized in figure (3) with an accuracy of 89.75917519% and an error rate of 10.24082481%.

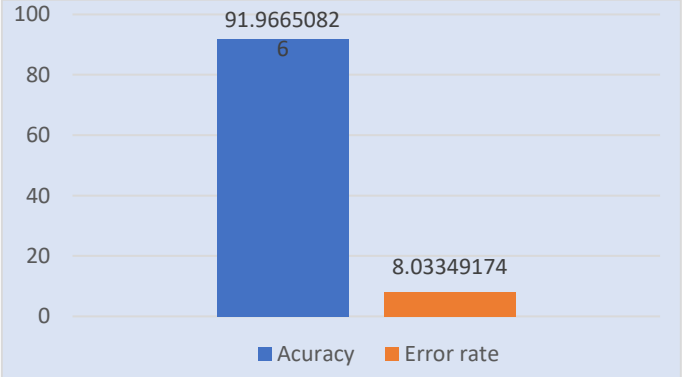

Figure 3. Random Forest with 10-Fold training results

The performance measurement Root Mean Square Error (RMSE) and Mean Absolute Error (MAE) has been summarized in Figure 4.

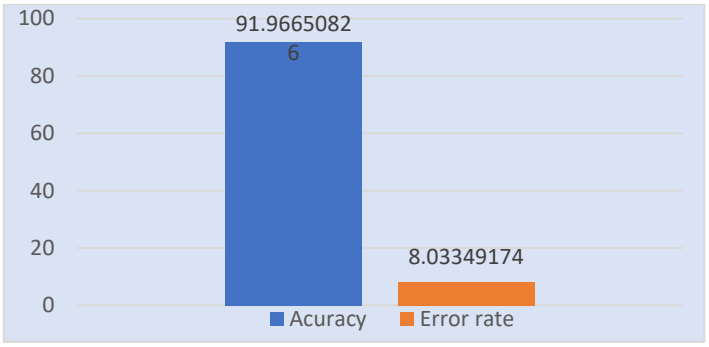

Figure 4. The performance measurements RMSE and MAE for Random Forest with the 10-Fold training set

2- Applying the Naïve Bayes technique with a training set of 66% and the remaining is the test set the result summarized in Figure 5 with the accuracy of 91.96650826% and an error rate of 8.03349174%.

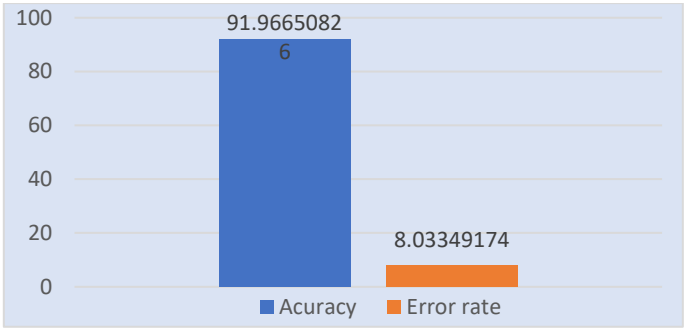

Figure 5. The results of Naïve Baes with 66% training set

The performance measurement Root Mean Square Error (RMSE) and Mean Absolute Error (MAE) for the Naïve Bayes technique has been summarized in Figure 6.

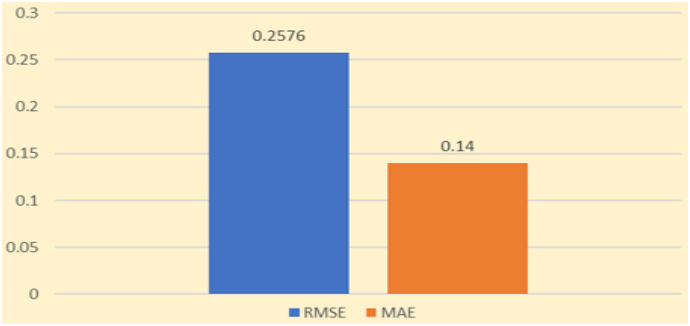

Figure 6. The performance measurements RMSE and MAE for Naïve Bayes technique with 66% training set

3- Appling Applying the Naïve Baye1Nearest Neighbor technique with a training set of 66% and the remaining is the test set the result summarized in Figure 7 with an accuracy of 94.68205476% and an error rate of 5.317945236%.

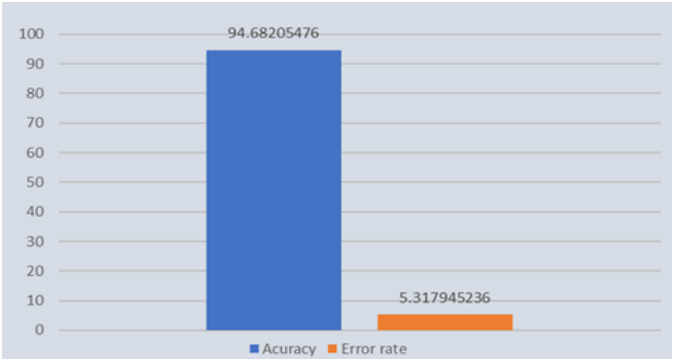

Figure 7. The results of 1 nearest neighbor with 66% training set

The performance measurement Root Mean Square Error (RMSE) and Mean Absolute Error (MAE) for the Naïve Bayes technique has been summarized in Figure 8.

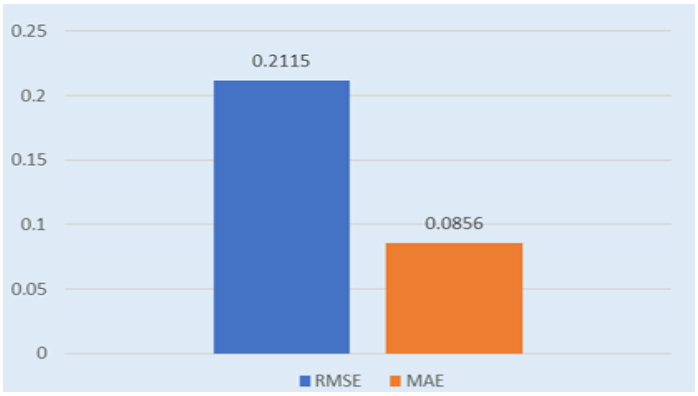

Figure 8. The performance measurements RMSE and MAE for 1 Nearest Neighbor technique with 66% training set

The summarization of the four ML techniques used in this research has been summarized in Figure 9.

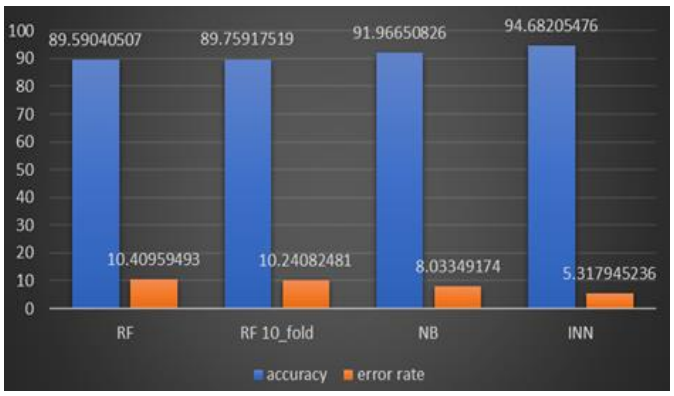

Figure 9. The summarization of accuracy and error rate of the four ML techniques.

5. Conclusion and future works

The research has some issues that should be discussed in this section:

- Random forest technique with a training set of 66% near to be equivalent with random forest with 10-Fold because the huge dataset and in the two cases have enough training.
- Feature selection methods do not work properly with such kinds of the dataset because of the data type of some features of the dataset.
- The ML model has been trained and tested using the five effective features date, user, source, action, and vector according to towards data science website.
- Body tracking, gait analysis using depth sensors will be added to the research in the future for purposes of confidentiality.
- As a future work also gesture recognition and body language can be added to discover the cases of lying and anxiety.

References

[1] Meritalk, "The 2017 federal insider threat report," Symantec, Tech. Rep., 2017. [Online]. Available: https://www.meritalk.com/study/ inside-job-the-sequel/

[2] Crowd Research Partners, "2018 insider threat report," 2018. [Online]. Available: https://crowdresearchpartners.com/insider-threat-report/

[3] CSO, U.S. Secret Service, CERT Division of SEI-CMU, KnowBe4, "The 2018 U.S. state of cybercrime survey," IDG, Tech. Rep., 2018. [Online]. Available: https://www.idg.com/tools-for-marketers/ 2018-u-s-state-of-cybercrime/

[4] M. L. Collins, M. C. Theis, R. F. Trzeciak, J. R. Strozer, J. W. Clark, D. L. Costa, T. Cassidy, M. J. Albrethsen, and A. P. Moore, “Common sense guide to mitigating insider threats, fifth edition,” The CERT Insider Threat Center, Tech. Rep. CMU/SEI-2015-TR-010, 2016.
[5] A. Azaria, A. Richardson, S. Kraus, and V. S. Subrahmanian, “Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data,” IEEE Trans. Comput. Social Syst., vol. 1, no. 2, pp. 135–155, Jun. 2014.
[6] M. H. Marx, "The general nature of theory construction," in Theories of Contemporary Psychology, London, MacMillan, p. 3–46, 1963.
[7] S. Messick, "Validation of inferences from persons’ responses and performances as scientific inquiry into score meaning," American Psychologist, vol. 50, pp. 741-749, 1995.
[8] M. T. Kane, "An argument-based approach to validity,"Psychological Bulletin, vol. 112, p. 527–535, 1992.
[9] I. Crinson, "Assessing the ‘insider–outsider threat’ duality in the context of the develop-ment of public–private partnerships delivering ‘choice’ in healthcare services: A socio-material critique," Information Security Technical Report, vol. 13, pp. 202-206, 2008.
[10] L. Coles-Kemp and M. Theoharidou, "Insider threat and information security management," in Insider threats in cyber security, Boston, Springer, pp. 45-71, 2010.
[11] J. Hunker and C. W. Probst, "Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques," JoWUA, vol. 2, no. 1, pp. 4-27, 2011.
[12] F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie and J. Cowley, "Analysis of unintentional insider threats deriving from social engineering exploits," in IEEE Security and Privacy Workshops, IEEE, pp. 236-250, 2014.
[13] R. Searle and C. Rice, "Assessing and Mitigating the Impact of Organisational Change on Counterproductive Work Behaviour: An Operational (Dis)trust Based Framework," The Centre for Research and Evidence on Security Threats (CREST), 2018.
[14] T. O. Oladimeji, C. K. Ayo and S. E. Adewumi, "Review on Insider Threat Detection Techniques," Journal of Physics: Conference Series, vol. 1299, p. 12046, 2019.
[15] D. M. Cappelli, A. P. Moore and R. F. Trzeciak, "The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes," Addison-Wesley Professional, 2012.
[16] J. R. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. Wright and M. Whitty, "Understanding insider threat: A framework for characterising attacks," in IEEE Security and Privacy Workshops, pp. 214-228, 2014.
[17] J. Glasser and B. Lindauer, "Bridging the gap: A pragmatic approach to generating insider threat data," in IEEE Security and Privacy Workshops, IEEE, pp. 98-104, 2013.
[18] M. R. Papandrea, "Leaker traitor whistleblower spy: National security leaks and the first amendment," BUL Review, vol. 94, p. 449, 2014.
[19] S. Mathew, M. Petropoulos, H. Q. Ngo and S. Upadhyaya, "A data-centric approach to insider attack detection in database systems," in International Workshop on Recent Advances in Intrusion Detection, Berlin, Springer, pp. 382-401, 2010.
[20] M. B. Salem and S. J. Stolfo, "Modeling user search behavior for masquerade detection," in International Workshop on Recent Advances in Intrusion Detection, Berlin, Springer, pp. 181-200, 2011.
[21] L. Laribee, "Development of Methodical Social Engineering Taxonomy. Master’s Thesis," Naval Postgraduate School, Amazon Digital Services, 2006.
[22] T. R. Peltier, Social Engineering: Concepts and Solutions, Information Systems Security, pp. 13-21, 2006.
[23] S. R. Band, D. M. Cappelli, L. F. Fischer, A. P. Moore, E. D. Shaw and R. F. Trzeciak, "Comparing insider IT sabotage and espionage: A model-based analysis (No. CMU/SEI-2006-TR- 026)," CARNEGIE-MELLON UNIV PITTSBURGH, 2006.
[24] R. A. Maxion, "Masquerade detection using enriched command lines," in In the Proceedings of the International Conference on Dependable Systems and Networks, pp. 5-14, 2003.
[25] J. E. Tapiador and J. A. Clark, "Masquerade mimicry attack detection: A randomised approach," Computers & Security, vol. 30, pp. 297-310, 2011.
[26] K. R. Sarkar, "Assessing insider threats to information security using technical, behavioural and organisational measures," Information Security Technical Report, vol. 15, pp. 112-133, 2010.
[27] O. Matters, "Insider Data Breach Survey 2019," Egress, 2020. [Online]. Available: https://pages.egress.com/rs/344-XTD- 684/images/egress-opinionmatters-insider-threat-researchreport-a4-uk-digital.pdf. [Accessed 2 Feburary 2020].

[28] R. Sanitioso, Z. Kunda and G. T. Fong, "Motivated recruitment of autobiographical memories," Journal of Personality and Social Psychology, vol. 59, pp. 229-241, 1990.
[29] M. L. Collins, M. C. Theis, R. F. Trzeciak, J. R. Strozer, J. W. Clark, D. L. Costa, T. Cassidy, M. J. Albrethsen, and A. P. Moore, "Common sense guide to mitigating insider threats, fifth edition," The CERT Insider Threat Center, Tech. Rep. CMU/SEI-2015-TR-010, 2016.
[30] National Cybersecurity and Communications Integration Center, "Combating the Insider Threat," The US Department of Homeland Security, Tech. Rep., 2014.
[31] L. Liu, O. De Vel, Q.-L. Han, J. Zhang, and Y. Xiang, "Detecting and Preventing Cyber Insider Threats: A Survey," IEEE Commun. Surveys Tuts., 2018.
[32] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, "Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures," ACM Computing Surveys, vol. 52, no. 2, pp. 30:1–30:40, Apr. 2019.
[33] K. Padayachee, "An assessment of opportunity-reducing techniques in information security: An insider threat perspective," Decision Support Systems, vol. 92, pp. 47–56, 2016.
[34] F. L. Greitzer and R. E. Hohimer, "Modeling human behavior to anticipate insider attacks," J. Strategic Security, vol. 4, no. 2, 2011.
[35] P. Legg, N. Moffat, J. Nurse, J. Happa, I. Agrafiotis, M. Goldsmith, and S. Creese, "Towards a conceptual model and reasoning structure for insider threat detection," J. Wireless Mobile Netw., Ubiquitous Comput., & Depend. Appl. (JoWUA), vol. 4, no. 4, pp. 20–37, 2013.
[36] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1153–1176, 2016.
[37] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools," IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 303–336, 2014.
[38] D. Caputo, M. Maloof, and G. Stephens, "Detecting insider theft of trade secrets," IEEE Security & Privacy Magazine, vol. 7, no. 6, 2009.
[39] P. Parveen and B. Thuraisingham, "Unsupervised incremental sequence learning for insider threat detection," in IEEE Int. Conf. on Intelligence and Security Informatics, 2012.
[40] T. Rashid, I. Agrafiotis, and J. R. Nurse, "A new take on detecting insider threats," in Int. Workshop on Managing Insider Security Threats, 2016.
[41] H. Eldardiry, E. Bart, J. Liu, J. Hanley, B. Price, and O. Brdiczka, "Multi-domain information fusion for insider threat detection," in IEEE Security and Privacy Workshops (SPW), 2013.
[42] G. Gavai, K. Sricharan, D. Gunning, J. Hanley, M. Singhal, and R. Rolleston, "Supervised and unsupervised methods to detect insider threat from enterprise social and online activity data," JoWUA, vol. 6, no. 4, pp. 47–63, 2015.
[43] H. G. Goldberg, W. T. Young, M. G. Reardon, B. J. Phillips, and T. E. Senator, "Insider threat detection in PRODIGAL," in Annual Hawaii Int. Conf. on System Sciences, 2017.
[44] T.E. Senator et al., "Detecting insider threats in a real corporate database of computer usage activity," in ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining (KDD), pp. 1393–1401, 2013.
[45] M. B. Salem and S. J. Stolfo, "Modeling user search behavior for masquerade detection," in Int. Symposium on Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, pp. 181–200, 2011. [46] F. Toffalini, I. Homoliak, A. Harilal, A. Binder, and M. Ochoa, "Detection of masqueraders based on graph partitioning of file system access events," in IEEE SPW, pp. 217–227, 2018.
[47] D. C. Le and A. N. Zincir-Heywood, "Machine learning based insider threat modelling and detection," in IFIP/IEEE Int. Symposium on Integrated Network Management, Washington DC, USA, 2019.
[48] S. C. Roberts, J. T. Holodnak, T. Nguyen, S. Yuditskaya, M. Milosavljevic, and W. W. Streilein, "A model-based approach to predicting the performance of insider threat detection systems," in IEEE SPW, 2016. [49] W. Meng, K. R. Choo, S. Furnell, A. V. Vasilakos, and C. W. Probst, "Towards bayesian-based trust management for insider attacks in healthcare software-defined networks," IEEE Trans. Netw. Service Manag., vol. 15, no. 2, pp. 761–773, 2018
[50] D. C. Le and A. N. Zincir-Heywood, "Evaluating insider threat detection workflow using supervised and unsupervised learning," in IEEE SPW, 2018.
[51] A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols, and S. Robinson, "Deep learning for unsupervised insider threat detection in structured cybersecurity data streams," in AAAI Workshop on Artificial Intelligence for Cyber Security, 2017.

[52] B. Bose, B. Avasarala, S. Tirthapura, Y. Y. Chung, and D. Steiner, "Detecting insider threats using radish: A system for real-time anomaly detection in heterogeneous data streams," IEEE Systems Journal, 2017.
[53] D. C. Le, S. Khanchi, A. N. Zincir-Heywood, and M. I. Heywood, "Benchmarking evolutionary computation approaches to insider threat detection," in ACM Genetic and Evolutionary Computation Conf., 2018.
[54] CERT Insider Threat Center, "The CERT Insider Threat Database," 2011, Available https: //insights.sei.cmu.edu/insider-threat/2011/08/thecert-insider-threat-database.html
[55] J. Glasser and B. Lindauer, "Bridging the gap: a pragmatic approach to generating insider threat data," in Proceedings of 2013 IEEE Security and Privacy Workshops, San Francisco, CA, pp. 98-104, 2013.
[56] K. Ball, "Workplace surveillance: an overview," *Labor History*, vol. 51, no. 1, pp. 87–106, 2010.
[57] J. Han and M. Kamber, Data Mining: Concepts and Techniques Second Edition. Elsevier Inc, 2006.
[58] P.-N. Tan, M. Steinbach, and V. Kumar, Introduction to Data Mining. Pearson Education Limited, 2014.