

SURVEY OF AI&ML IN THE TERRAIN OF CYBERWARFARE ON FINANCIAL INFRASTRUCTURE

R MANOJ KUMAR

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

{CYBER SECURTIY AND DIGITAL FORENSICS}

VIT BHOPAL

MARCH 2024

**Abstract -** As the number of cyber crimes keeps on increasing with evolving technology it is equally important to upgrade our systems and networks to prevent it.This paper explores the growing significance of artificial intelligence in a situation of cyberwarfare associated to the domain of financial infrastructure. Formulating the process of using sandbox with machine learning. We used hidden Markov model for feature engineering .We also have reviewed threat detection framework for ml model.

Keywords: vulnerabilities, malware,artificial intelligence,cyberwarfare,data,financial infrastructure

**INTRODUCTION**

Cyber warfare targeting financial infrastructures pose a significant threat in the digital age .As financial systems become more technologically complex and connected,they are exposed to wide range of attacks and disruption leading to data theft,economic disruption,undermining of public trust .Financial institutions like banks ,stock exchanges and payment processors are attractive targets for cyber attackers due to the vast amounts of valuable data they handle

The focus is to develop a sophisticated counter measure system to deal with the attacks, but the process must be in work all the time. This is possible by automating functions like intrusion detection systems,behavioral analysis,anamoly detection, incident response,and multi-factor authentication with the help of AI.

Being a victim of a cyberwarfare involves a lot of catastrophic impacts that follows .Most of the time it would be data breaches,thefts,disruption of services,market manipulation which may result in escalation of conflicts,loss of reputation and wealth,violation of legal compliance,or sometimes even permanent dis-function of organization.

The implementation of AI in preventing cyber warfare continues to evolve rapidly.In the current scenario AI based systems like Threat detection and prediction,automated incident response, behavioral analysis and anamoly detection ,adaptive security measure and threat intelligence analysis models are under devepment. This is possible due to the increasing adoption and innovation across various cyber domains ,however it is essential to continue advancing AI in combating against cyber warfare.

The primary motivation is to develop modern age defensive systems against cyberwarfare.This development would also signify the nations capability in terms of technolgy ,research and advancements , preventing attacks under all circumstances.

.

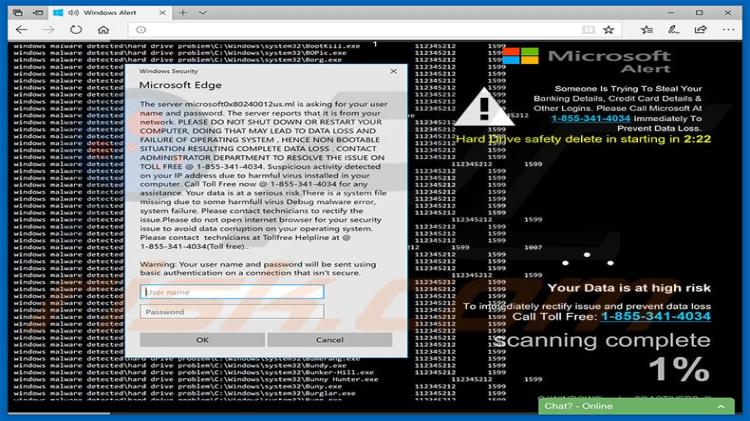


Fig 1.1 malware detecting software

**LITERATURE REVIEW**

In the paper [1] “A Brief Summary of Cybersecurity attacks in V2X Communication” by N. Mazher, M. Alhadaad, and O. Shagdar discuss about the technology of v2x and leading potential security threat in it .The paper involves collecting data from cloud,iot and web and creating a ml model involving regression for observing abnormal activity or false injunction.

In paper [2] “AI Revolutionizing Cyber security unlocking the Future of Digital Protection” by A. Lakhani discuss the various ways in which AI is revolutionizing cybersecurity.It highlights AI's ability to analyze vast amounts of data, detect patterns, and identify anomalies. The author uses AI framework to detect and respond to cyber threats in real-time, significantly reducing response time and minimizing potential damage.

In the paper[3] “A machine learning approach to detecting senior data modification intrusion in WBANs” by A.Verner and D.Butvinik, In WBAN only little quality of the answers are produced, the best are code blue and alarm net. In this field it uses the similar method of enlisting the received data in an efficient format in many fields.The keys used are ‘Assumptions, method, Chosen ML features, chosen structure of negatively labeled vector’ which are the key tools used in the study. The studying phase of SVM and also the execution time have taken longer period to complete in a way many of the vectors were combined to overcome the drawback of the time with a complete accuracy level. Still better modification is in need for this method

In the paper [4], ‘Machine learning to detect anomalies in web log analysis’ published by Q.Cao, Y.Qiao, and Z.Lyn..This paper segregates the whole system into 4 different parts are ‘data pre-processing, decision free classifier, data extractor, Hidden Markov model’ are the included models. It mainly relates in producing the solutions in a path of data.This proposed method builds a proper model for regular files and then maintain them as the detector. This paper produced high level of optimum solution of about 93% and negative positive rate till 4%.

In the paper [5], ‘Evaluation of machine learning techniques for network intrusion detection’ by M.Zaman and C.H.Lung, have mentioned that in the evaluation of machine learning for detection clustering types are mostly utilized. The paper totally represented six separate methods of machine learning along with six ensemble methods which is used to gather the results for the attacks. But when compared with the ROC results, it was not satisfactory although it had opened a unique route of machine learning. The technique involved in tracking the traffic data which had involved true positive, false positive, true negative and false negative. The proposed method did not provide better 240 results hence further study and adaptable measure is a must in the future studies.

In the paper [6] ‘A review of intrusion detection using anomaly based detection’ by authors U.Kumari and U.Soni, have illustrated that the most important aspect of data security is data intrusion detection, in identifying the fraud, fake products, attacks. This intrusion is used to detect the attack cause or the root or the relation/bridge between the huge set back of attack. The unusual patterns can be easily identified for any terrorist activities as the data attack. This paper has improved the effectiveness of the system functionalities also with the secure feature. The huge drawback is that in securing the database the paper has left out [5].

1. **CYBER VIGILANCE REDEFINED: UNLEASHING AI FOR THREAT PREDICTION AND PREVENTION**

Cyber threat is a broad problem with immense challenges and consequences ,

Growing need of stronger and advance cyber security systems.

Using AI and ML to detect threats like malware's, data thefts by phishing

Increasing security and safety of sensitive data s ,decreasing vulnerabilities to attacks.producing better threat detection and termination system.

**2.1 Data collection**

There are multiple kinds of data from various sources which is involved in the data collection process .Some of them are system logs from servers,workstations,applications and other IT infrastructure components. These can provide valuable information on security breaches.Data can be gathered from endpoints , which can give us the signs of unauthorised access , malware injection or unusual file activity. The installed security devices can also provide data regarding detected threats, blocked connections and security policy violation.Apart from these. Data can also be extracted from other sources like cloud services, user behaviour analytics and external threat intelligence feed

Some of the methods involved in exraction includes deploying agents,NIDS,API integration,scanning and crawling [2].

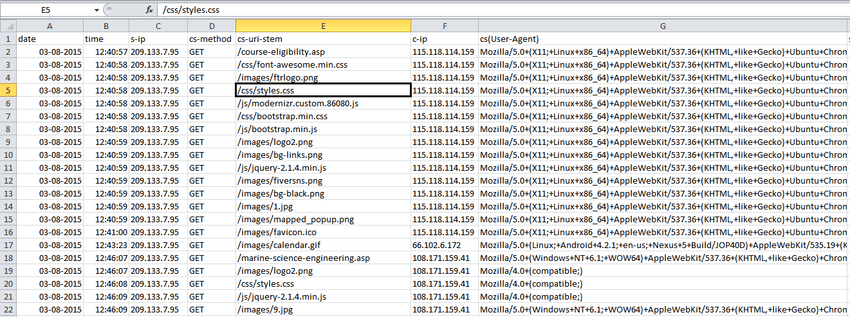


Fig.1.2 logs data of a finance company

**2.2 Data Reprocessing**

The first step involves cleaning data by eliminating duplicates ,removing or correcting any inconsistencies,errors or missing values in the dataset **Fig1.1**. This is followed by normalization using min\_max scaling and z-score normalization. From the collected data features are identified and analyzed. These features are then converted to numerical form by label encoding,while some of the features can be newly created by feature engineering for greater predictive performance. Finally by using techniques of dimensionality reduction such as PCS or t-SNE we can visualize and identify patterns in high dimensional data

**2.3 Feature Engineering**

It is crucial to exract relevant information from the data.Analyzing transaction volume over time to identify abnormal spikes or dips that could indicate fraudulent activity.[15]Observing Transaction frequency and amounts for individual accounts across the systems to detect unusual patterns.Examining geographical location, account activity , time ,login frequency to study the patterns and generating anomoly scores for each feature based on histrorical data and use these to flag unusual patterns.

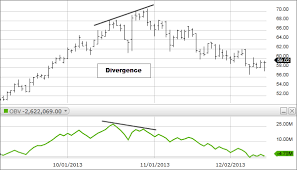
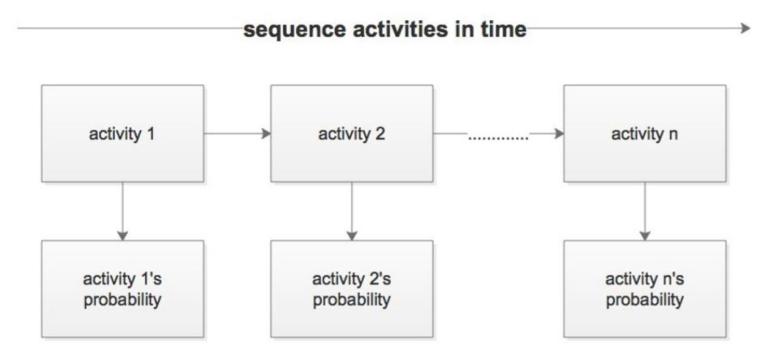


Fig 1.3 Divergence simulation graph

### **Hidden Markov Model**

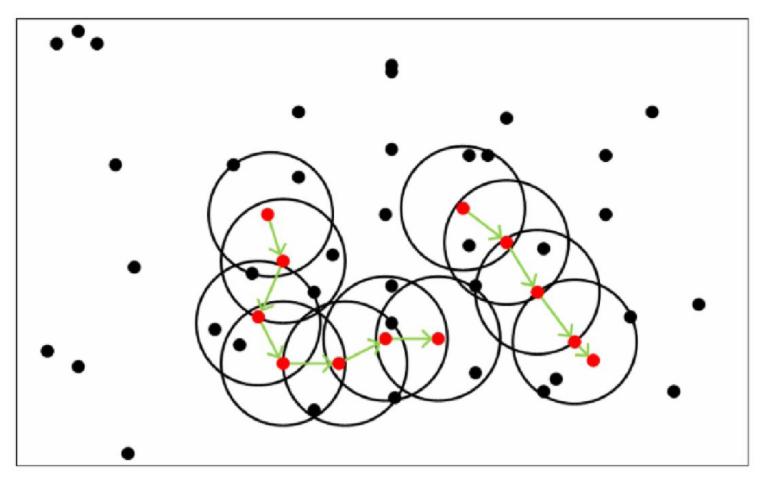
An HMM is a statistical Markov model in which the system being modeled is assumed to be a Markov process with unobserved (hidden) states [16]. A Markov model can simple to understand as defining the probability of each behavior occurring and then identifying the product of the possibilities of all actions arising over a period. A simple Markov model’s structure is shown in **[Figure 1](https://www.ijfis.org/journal/view.html?uid=901&page=&pn=mostread&sort=publish_Date DESC&spage=&vmd=Full" \l "F1" \o ")**.4 By comparison, when the sequence is relatively long, it isn’t straightforward for the Markov chain to distinguish several behaviors. Because HMM has a hidden layer, it is easier to distinguish between normal and abnormal behavior than the Markov chain

Fig 1.6 Representing Hidden Markov Model

### **DBSCAN**

DBSCAN is a data clustering algorithm proposed by Ester, et al. [10] in 1996. The method used by DBSCAN is straightforward. It arbitrarily selects a core object without a category as a seed and then finds all the sample sets whose core objects can reach a density, which is a cluster. Then continue to select another core object without a category to find a sample set with a dense density to obtain another clustering cluster. Run until all core objects have categories.

It can be easily seen from [Figure 1.7](https://www.ijfis.org/journal/view.html?uid=901&page=&pn=mostread&sort=publish_Date DESC&spage=&vmd=Full" \l "F7" \o "). that the above definition is understood. In [Figure1.7](https://www.ijfis.org/journal/view.html?uid=901&page=&pn=mostread&sort=publish_Date DESC&spage=&vmd=Full" \l "F7" \o "), MinPts = 5, the red points are the core objects because their e-neighborhood has at least 5 samples. The black samples are non-core objects. All samples with linear core object density are in the hyper sphere with the red core object as the center. If they are not in the hyper-sphere, they cannot be directly dense. The core objects connected by the green arrows in [Figure 1.7](https://www.ijfis.org/journal/view.html?uid=901&page=&pn=mostread&sort=publish_Date DESC&spage=&vmd=Full" \l "F7" \o "). form a sample sequence with a density. All samples in the ε-neighborhood of these dense sample sequences are densely connected.

Fig 1.7: DBSCAN illustration

**3 METHODOLOGY AND DESIGN**

* 1. **Approach**

The approach to developing the expanded threat model is to build on the threat modeling framework and high-level threat model presented in [12]. Section 3.1 reviews the framework, draws well-established repositories of adversary TTPs and attack patterns

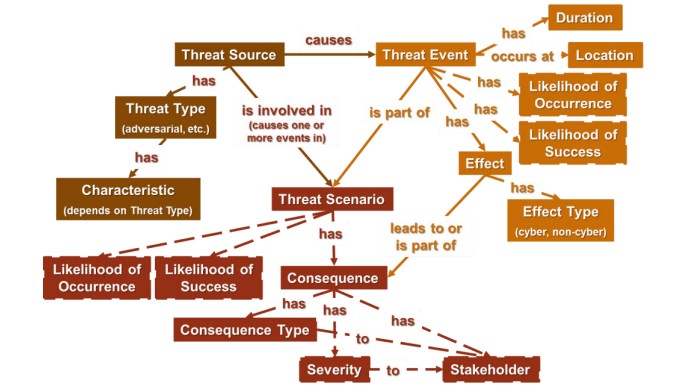


Fig 1.8 Threat modelling framework

The high-level threat modeling framework is based on the National Institute of Standards and Technology (NIST) 800-30R1 framework [4], elaborated and fusing in material from other frameworks to meet the needs of NGCI Apex. It provides representative values for key constructs and relationships and describes how threat scenarios can be generated from the framework. Constructs and relationships in dotted lines are included to indicate linkages to risk modeling. While they are not part of the threat model presented in this report, these constructs are used in risk assessment, and relate to the system model or the asset model which is part of a detailed threat model.

* 1. **ARCHITECHTURE MODEL FOR CYBER SECURITY USING SAND BOX**

For machine learning algorithms to achieve a better performance it is necessary to run the malware in a sandbox to collect features from the malware which cannot be obtained statically. We present a novel architecture model based on machine learning for the prediction of malware that requires execution in a sandbox environment. In Figure 1.9 Network-based anti-malware gateway i.e. sandbox deployment led to widespread exposure of antivirus weaknesses resulting in a wave of next-generation endpoint security deployment as well as industry innovation. The goal of machine learning based architecture is to make predictions on the unseen data and present a final model that performs the finest job defined by parameters like available historical data, the time spent on the architecture and finally the procedure.Data from enterprise internet is collected for classification, i.e. the data is identified in two forms one is bad data and the other is, data for training set containing both positive and unlabelled data set. Problems which involve classification are considered as part of machine learning. In machine learning (ML) the computer gets the ability to learn from data. After the data is classified it is segregated into groups using clustering, on certain set of rules. This can be achieved by applying clustering models (Centroid, distribution and connectivity) [17].Clean data is moved directly to sand box as test data for further deep malware detection. The primary requirement of training dateset is that it must be accurately labelled as it may predict misleading results and the future unknown sample of data. The training set containing one labeled and another unlabeled data set (positive data (labeled) as well as malicious sample (unlabeled)) [18 ] is applied to the training model. Now the rules are extracted from these trained data set. These rules are used to train the algorithm. Principally, this leads to the creation of classifier for new samples. Here training data is prepared to train the model by applying it to various filters.

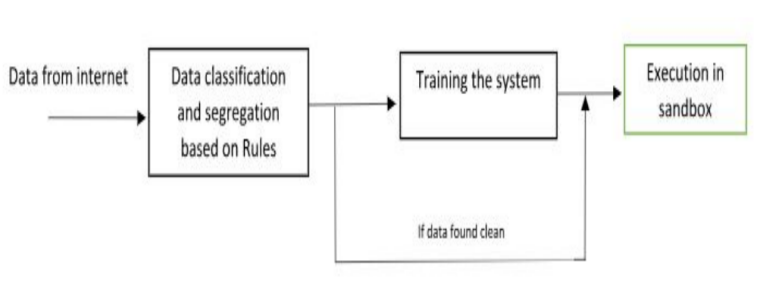


Fig 1.9 Threat Detection Model

The unknown sample of data is provided to the training model for its detection. The training set creates a model which understand the success rate of input data set. In fig 2.0 as below shows in detail the training model. It shows how it detects the malicious threats based on certain set of rules that are selected on the basis of trained set. As shown in figure 2.0 below. The output from trained database model is in the form of decision or metric. The decision from user is taken in the form of true or false from user. If rules does not match (false), the sample data is send to training the database for adding new rules. After rule matches, that pure data is sent to database for storing.

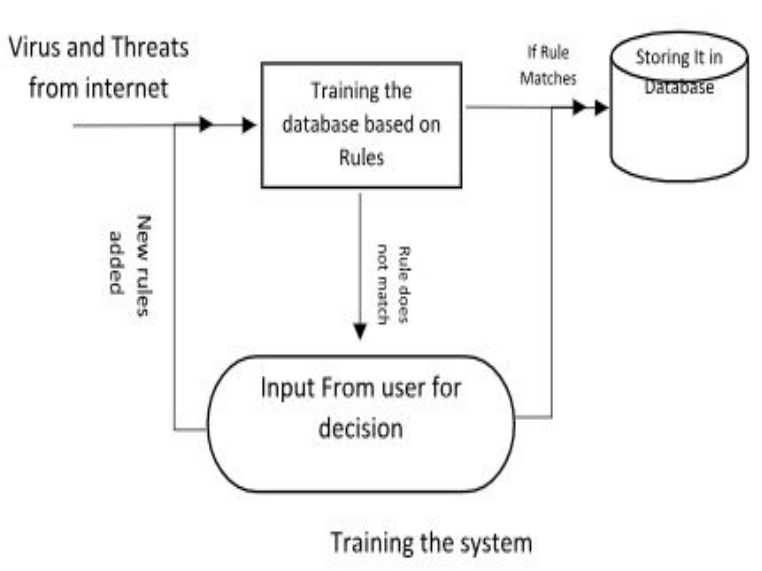


Fig 2.0 Training the system

From database it will go to sandbox as in figure 1.9. Another powerful tool for advance threat detection is Sandbox. Sand-boxing along with machine learning methods has emerged as a powerful cyber security tool. The time taken by the algorithm to train a database (i.e., training time) varies from algorithm to algorithm. Lots of research is needed for selecting the ML algorithm according to application. Area like if the input is continuous apply supervised machine learning methods and if discrete apply unsupervised learning methods. The selection of algorithm also depends upon the working mode (online or offline) of a security analytic system. It is clear that to apply the machine learning algorithms to any problem, it is essential to represent the data in some form. For this purpose, Sandbox is used. The reports generated by the sandbox, describing the behavioral data of each sample, are per-processed, and malware features are extracted from there [19 ]. Sand boxing engages in the capturing a document or executable file which is then opened within a secure virtual machine. In this controlled environment, in order to observe how the executing software behaves exactly, potential threats are run. Sandbox is used for executing untrusted, untested programs or code, possibly from unverified third parties, websites, suppliers, without risking any harm to the host machine in cyber-security system or any operating system. An advanced sand-boxing solution provides CPU-level threat protection which depends on the mishandling stage of the attack. This allows an organization to be detected and blocked against advanced persistent threats (APT). A software architect should take into consideration several things during the selection and integration of an optimized algorithm. The ML algorithm performs better for one type of security analytics (e.g., detecting DOS attack) may not perform well in another security analytics i.e detecting brute force attack). The selection of an algorithm is tricky in a way that if it is giving performance, then it may degrade other system qualities like accuracy, complexity, and understand ability of the final result. For example, Researchers [21] compared SVM (Support Vector Machine) with Extreme Learning Machine (ELM) in terms of accuracy and performance. It is found out that SVM (Support Vector Machine) produced more accurate results but proved computationally expensive. On the other hand, ELM proved lighter but produced less accurate results. A practical trade-off should be recognized while selecting the algorithm among various system’s qualities. As it is said in paper[20] “While there is no silver bullet to solve the cybersecurity challenge, the key is to use layered defenses along with machine learning threat detection capabilities for optimum results".

1. **RESULTS OF APPLYING MACHINE LEARNING IN CYBER SECURITY**

These are the threats that ML can save against [38]:-

1. Ransomware- malware that dont allows the user to access its personal files and ask for ransom payment for again accessing personal account.
2. Watering Hole- Hackers in this keep on tracking the websites on which users usually visits and access their identification is the concept of a watering hole.
3. Web shell - Web shell is a short code that allows the hacker to make modifications on server's web root directory. This means that full access to the database of the system is gained. If it is an e-commerce website, in order to collect credit card information of the customer who operates on everyday can access the database.

4. Spear Phishing- The Machine learning trained models can be used to detect whether the email is malicious or not by identifying the key features such as email headers, subsamples of body-data, punctuation patterns, etc.

1. **CONCLUSION**

Through this paper we came across varies process involved in understanding and analyzing the threat associated to cyber attacks .The paper also covers process of collecting data, processing data and feature engineering .We also modeled a framework for designing a threat model. Applying this technique proves to be an efficient and autonomous in advance threat detection systems.We used sandbox with machine learning on the model which has proven to be a powerful method for advanced threat protection

[1]N. Mazher, M. Alhadaad, and O. Shagdar, "A Brief Summary of Cybersecurity attacks in V2X Communication," 2022.

[2]A. Lakhani, "AI Revolutionizing Cyber security unlocking the Future of Digital Protection," 2023, doi: https://osf.io/cvqx3/.

[3] “A machine learning approach to detecting senior data modification intrusion in WBANs” by A.Verner and D.Butvinik mar23 2022.

[4]R. Talwar and A. Koury, "Artificial intelligence–the next frontier in IT security?," Network Security, vol. 2017, no. 4, pp. 14-17, 2017.

[5]A. Lakhani, "Enhancing Customer Service with ChatGPT Transforming the Way Businesses Interact with Customers," 2023, doi: https://osf.io/7hf4c/.

[6]C. R. Moran, J. Burton, and G. Christou, "The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying," Journal of Global Security Studies, vol. 8, no. 2, p. ogad005, 2023.

[7]J. Nsoh, "“NEXT-GEN” CYBERSECURITY," 2021.

[8]T. J. Ramdass, N. Munshi, R. Kim, and G. Falco, "Cybersecurity of On-Orbit Servicing, Assembly, and Manufacturing (OSAM) Systems," in ASCEND 2022, 2022, p. 4379.

[10]. Ester, M, Kriegel, HP, Sander, J, and Xu, X 1996. A density-based algorithm for discovering clusters in large spatial databases with noise., Proceedings of the 2nd International Conference on Knowledge Discovery and Data Mining (KDD), Portland, OR, pp.226-231.

[11] J. E. Rubio Cortés, "Analysis and design of security mechanisms in the context of Advanced Persistent Threats against critical infrastructures," 2022.

[12] Bodeau, D., McCollum, C., and Fox, D. 2018. “Cyber Threat Modeling: Survey, Assessment, and Representative Framework,” HSSEDI, The MITRE Corporation, 2018.

[13] S. A. Talesh and B. Cunningham, "The Technologization of Insurance: An Empirical Analysis of Big Data an Artificial Intelligence's Impact on Cybersecurity and Privacy," Utah L. Rev., p. 967, 2021.

[14] E. Fosch-Villaronga and T. Mahler, "Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots," Computer law & security review, vol. 41, p. 105528, 2021

[15]. Xiaoyun Ye , Sung-Sam Hong , and Myung-Mook Han Department of Computer Science, Gachon University, Seongnam, Korea . “Feature Engineering Method Using Double-Layer Hidden Markov Model for Insider Threat Detection” February 28, 2020. [16].Ghahramani, Z (2001). An introduction to hidden Markov models and Bayesian networks. International Journal of Pattern Recognition and Artificial Intelligence. 15, 9-42. [https://doi.org/10.1142/S0218001401000836](https://doi.org/10.1142/S0218001401000836" \t "https://www.ijfis.org/journal/_blank) [17]. S. B. Kotsiantis, “Supervised Machine Learning: A Review of Classification Techniques”, Published in Proceedings of the 2007 conference on Emerging Artificial Intelligence Applications in Computer Engineering Real Word AI Systems with Applications in eHealth, HCI, Information Retrieval and Pervasive Technologies, IOS Press Amsterdam, The Netherlands, The Netherlands, pp. 3-24, ISBN: 978-1-58603-780-2, 2007. [18] Anoop Kumar Jain and Satyam Maheswari, “Survey of Recent Clustering Techniques in Data Mining”, International Archive of Applied Sciences and Technology, Volume 3 [2], ISSN: 0976-4828, pp. 68 - 75, June 2012. [ 19 ] B. Liu, X. Li, W. Lee, & P. S. Yu, “Text Classification by Labeling Words. Retrieved”, American Association for Artificial Intelligence, 2004. [ 20 ] L. Vokorokos, A. Balaz and B Mados, “Application Security through Sandbox Virtualization”, Acta Polytechnica Hungarica, Vol. 12, No. 1, 2015.

[ 21 ] R. Caruana and A. Niculescu-Mizil, "An empirical comparison of supervised learning algorithms", Proceedings of the 23rd international conference on Machine learning - ICML '06, 2006.