MACHINE LEARNING APPROACH TO IDENTIFY THE MAN IN THE MIDDLE ATTACK.

[1]Mr. S Pavan Kumar Reddy, [2]Mrs. K Anuranjani, [3]Mr. P Anvesh Reddy
[4]Mr. V Bhuvana Chandra, [5]Mr. C Aniketh

[2]Assistant Professor
Dept of CSE
Bharath University,
Chennai.

***Abstract*- We can better grasp how the threat environment has evolved by analyzing data sets on cyber incidents. We learn about numerous cyber breaches and hacking incidents that occur today. In this project, we look at the numerous cyber-attacks and breaches, analyze how they are carried out, and come up with a replacement. We demonstrate that since these attacks include autocorrelations, we should characterize both the hacking breach incident inter-arrival periods and breach sizes using stochastic processes. We come to a few conclusions about cyber security, one of which is that the threat posed by hacker attacks is indeed increasing. The algorithms Convolution Neural Network (CNN) and Recurrent Neural Network (RNN) will be used in our study to analyze the findings.**

I. INTRODUCTION

An information break is the intentional or unintentional transfer of secure or private/classified data to an untrusted domain. An information rupture is a security incident in which delicate, ensured or secret information is copied, transmitted, seen, stolen, or used by a person not authorized to do as such. Inadvertent data disclosure, information spill, and further information spill are more terms for this wonder. This may include incidents like theft or loss of modern media like computer tapes, hard drives, or smart phones—media where such data is stored decoded—posting such data online or on a computer generally accessible from the Internet without legal data security safeguards, and transferring such data to a framework that isn't completely open but isn't properly or formally authorized for security at the affirmed dimension, like decoys. While technological solutions can defend digital systems from attacks, information leaks continue to be a serious problem. This motivates us to explain how information rupture events develop. This will not only increase our understanding of information breaches but also clarify various damage-reduction strategies, such as protection. Many people believe that protection will be beneficial, but the development of precise cyber risk measurements to manage the task of protection rates is outside the bounds of the current understanding of information breakdowns. We take the corresponding promises in this document. We argue that in order to demonstrate both the hacking break occurrence entomb entry timings and rupture sizes, stochastic approach should be used instead of circulating the ruptures. We show that these stochastic method models can predict the relationship between landing times and rupture sizes. To the best of our knowledge, this is the first work to argue that stochastic methods, rather than circulations, should be used to demonstrate these digital risk elements. We show that a particular copula can accurately represent the dependence between the episode's entry time and the break sizes.

These are the key pieces illustrating both the existence of this reliance and the consequences of ignoring it. We also show that it is crucial to consider the dependency when predicting entomb entrance times and break sizes because in most cases, the results are inaccurate. We anticipate that the current study will spark further research that can provide in-depth understanding of other risk mitigation strategies. Because they must thoroughly and comprehend the nature of data breach risks,insurance companies, governmental organizations, and regulators can benefit from these insights. We anticipate that the current study will spark further research that can provide in-depth understanding of other risk mitigation strategies. Because they must thoroughly comprehend the nature of data breach risks, insurance companies, governmental organizations, and regulators can benefit from these insights.

II. RELATED WORKS

Different relative analysis was conducted using various classification schemes, however no one methodology stood out above the rest. Finding the ideal classification scheme involves looking at issues including consistency, workout duration, scalability, and many more.

Dougan Aksu ; M. Ali Aydin Have developed algorithms such as Intrusion Detection Systems (IDS) to avoid cyber-attacks. In this study, deep learning, and support vector machine (SVM) algorithms were used to detect port scan attempts based on the new CICIDS2017 dataset and 97.80%, 69.79% accuracy rates were achieved respectively.

Fouzi Benamar Bouyeddou ; Ying Sun ; Benamar Kadri have designed CRPS monitoring approach which helps in detecting TCP SYN flood attacks. The efficiency of the proposed methods has been verified using the 1999 DARPA intrusion detection evaluation datasets. Evaluation datasets.

Hanan Hindy ; Elike Hodo ; Ethan Bayne ; Amar Seeam ; Robert Atkinson ; Xavier Bellekens proposed a taxonomy for classifying network attacks in a consistent way, allowing security researchers to focus their efforts on creating accurate intrusion detection systems and targeted datasets.

James Weimer ; Radoslav Ivanov ; Sanjian Chen ; Alexander Roederer ; Oleg Sokolsky ; Insup Lee mentioned the consiquences of using CPS and designed parameter-invariant (PAIN).. PAIN monitors are designed such that unknown events and system variability minimally affect the monitor performance. This work describes how PAIN designs can achieve a constant false alarm rate (CFAR) in the presence of data sparsity and intra/inter system variance in real-world CPS.

Firas Saidi ; Zouheir Trabelsi ; Henda Ben Ghazela has suggested the article that illustrates how social media and networking playing roles in cyber-attacks and proposed. cyber community detection approach based on Constrained Evidential C-Means (CECM) algorithm which is an adequate evidential clustering method that can be applied to detect cyber terrorist subgroups.

Dawei Shi ; Ziyang Guo ; Karl Henrik Johansson ; Ling Shi IEEE 2022. have mentioned the problem of attack detection in cyber physical systems. Transfer entropy-based causality countermeasures are introduced for both sensor measurements and innovation sequences. The effectiveness of the transfer entropy countermeasures in attack detection is evaluated via theoretical analysis, numerical demonstrations, as well as comparative simulations with classical χ 2 detectors.

Koji Nakao. have mentioned on how malwares triggering to cyber-attacks. passive monitoring technologies were used to proactive the cyber security response. Future security considerations will be given for utilizing extendible passive monitoring technologies to proactively respond against cyber-attacks under smarter city and connected environments.

Abu Shakil Ahmed ; Sudip Deb ; Al-Zadid Sultan Bin Habib ; Md. Nurunnabi Mollah ; Abu Saleh Ahmad suggested a framework for both automatic and manual techniques have been proposed to detect cybercrime and charge the offender with proof.

IbtissamBenchaji ; Samira Douzi ; Bouabid ElOuahidi. have enhanced classified performance of the minority of credit card fraud instances in the imbalanced data set, for that they propose a sampling method based on the K-means clustering and the genetic algorithm.

Al-Sakib Khan Pathan. have suggested the way to defend against common cyber-attacks through phishing and cross-site scripting.

III. DP CONCEPT

Cybercrime is also on the rise as a result of the expansion of the Internet. Internet crime has many faces and is carried out in a variety of ways. Cybercrime is the term used to describe crimes that involve computers and the internet. Cybercrimes are a result of the internet's development and global variety. Essentially, there are two main types of cybercrime. One of those views the network as a potential target for criminal activity, including hacking and system destruction. The other group consists of those who use networks to perform crimes like fraud. Even though the term "cybercrime" is now widely used, it is difficult to define precisely. In their definition of cybercrime, Somaiya et al. state that the term "cybercrime" is "a term that is widely used to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity." Cybercrimes also include illegal activities carried out on computers, such as virus attacks, financial crimes, the sale of illegal goods, the promotion of pornography-sex videos, online gambling, e-mail spamming, cyber phishing, cyber stalking, unauthorized access to computer systems, the theft of data stored in electronic form, e-mail bombing, physically damaging computer systems, etc. The figures that have been gathered and discussed show how severe Internet crimes are globally. Just "phishing" emails themselves bring in $1 billion for their authors. 90 percent of the 500 organizations polled by the FBI in early reported security breaches, and 80 percent of those claimed financial losses. According to a national report from 2018, four billion dollars are lost due to credit card theft each year. Only 2% of credit card transactions are made online, but 50% of the four billion transactions mentioned earlier come from online transactions. These findings provide as a concrete example of how the Internet is being abused and serve as justification for the need to slow down online crime.

The fundamental thrust of this idea is that most of our daily conversations and business transactions now occur online because we live in a globally interconnected internet environment. Threats in cyberspace move at the speed of light because cyber infrastructure is extremely vulnerable to attacks. The protection of cyberspace cannot be handled by any physical device or by human involvement alone due to the speed and volume of data used in it. To identify dangers and make wise judgements in real time, there must be a significant amount of automation. It is challenging to create / make software with traditional algorithms that can effectively defend against the threats that are continually changing. By incorporating artificial intelligence approaches into the software, it can be overcome. This study's goal is to investigate how artificial intelligence might be used to combat cybercrime. The following are the project's primary focuses:

1. To determine how well cybercrime incidents are predicted.
2. To learn the specifics of the crime's motive.
3. All datasets should be usable with our research.

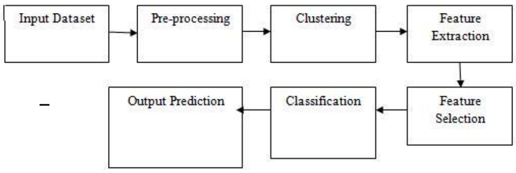

Fig.1. Disparity in existing system architecture.

IV. METHODOLGIES

The system will look at how to convert crime information into a data-mining problem, so that it will help detectives in solving crimes faster Crime analysis based on available information to extract crime patterns. Using various data mining techniques, frequency of occurring crime can be predicted based on territorial distribution of existing data Crime recognition. A recurrent neural network (RNN) is a class of artificial neural networks where connections between nodes form a graph along a temporal sequence. This allows it to exhibit temporal dynamic behavior. Derived from feed forward neural networks, RNNs can use their internal state (memory) to process variable length sequences of inputs. This makes them applicable to tasks such as unsegmented, connection.

The term "recurrent neural network" is used indiscriminately to refer to two broad classes of networks with a similar general structure, where one is finite impulse and the other is infinite impulse. Both classes of networks exhibit temporal dynamic behavior. A finite impulse recurrent network is a directed acyclic graph that can be unrolled and replaced with a strictly feed forward neural network, while an infinite impulse recurrent network is a directed cyclic graph that cannot be unrolled. Both finite impulse and infinite impulse recurrent networks can have additional stored states, and the storage can be under direct control by the neural network. The storage can also be replaced by another network or graph, if that incorporates time delays or has feedback loops. Such controlled states are referred to as gated state or gated memory, and are part of memory networks (LSTMs) and gated recurrent units. This is also called Feedback Neural Network (FNN).

Proposed System Advantages:

- High output efficiency.
- User friendly.
- Less time consumption.
- Can be implemented in all datasets.
- Early prediction of crimes is possible.

V. PROCEDURE EVALUATION

1. Input dataset:

Dataset can be taken from online source provider called UCI repository. We have collected set of criminal datasets which we are going to analyze. Then for training the data set also for the comparison of the non-criminal datasets are also been taken.

2. Analysis of data set:

Here the analysis if dataset takes place. The size of data is taken into consideration for the data process.

3. Oversampling (Using SMOTE): we have created a detailed history of all crimes that been complained over a certain amount of time and it is sampled to fix a threshold value.

4. Training and Testing Subset: As the dataset is imbalanced, many classifiers show bias for majority classes. The features of minority class are treated as noise and are ignored. Hence it is proposed to select a sample dataset.

5. Applying algorithm: Following are the classification algorithms used to test the sub-sample dataset.

a. Convolution Neural Network (CNN) and b. Recurrent Neural Network (RNN)

6. **Predicting results:** The test subset is applied on the trained model. The metrices used is accuracy. The ROC Curve is plotted and the desirable results are achieved.

7.

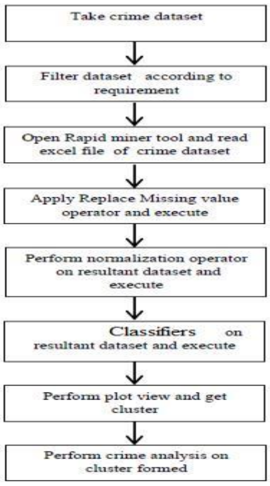
Take crime dataset
Filter dataset according to requirement
Open Rapid miner tool and read excel file of crime dataset
Apply Replace Missing value operator and execute
Perform normalization operator on resultant dataset and execute
Classifiers on resultant dataset and execute
Perform plot view and get cluster
Perform crime analysis on cluster formed

Fig.2. Flow diagram of our proposed system.

VI. CONCLUSION

The widespread of ordinary data breaches around the world demonstrates how real the danger of critical infrastructure attack as the hackers increase in terms of sophistication and technical expertise, and as the critical information infrastructure becomes more massive and intricate, it is more vulnerable to attack. We can treat them like an act of terrorism which justifies action under the Internal Security Act. If we take this path, we must be prepared of the consequences. What is more compelling is the need to strengthen the security itself. As illustrated in this article, a multi -prong action is required; one that involves a mixture of technology, competency of manpower, prudence, and effective legal framework. At this end, it is note-worthy that there are few areas emerged from this initial study that can be made an agenda of future direction. Firstly, from the technical perspective, there is a need to assess new methods that threaten the security of critical information infrastructure. Secondly, from the perspective of law and policy, governments need to ensure that each sector identified as critical infrastructure should be properly protected both by legal and policy instruments.

REFERENCES:

1. Cheshta Rani, Shivani Goel. An Expert System for Cyber Security Attack Awareness, International Conference on Computing, Communication and automate /Automation (ICCCA2015) ISBN:978-1-4799-8890-7/15/$31.00 ©2015 IEEE 242 CSAAES.
2. A. S. Poonia, A. Bhardwaj, G. S. Dangayach, (2011) “Cyber Crime: Practices and Policies for Its Prevention”, The First InternationalConferenceon Interdisciplinary Research and Development, Special No. of the International Journal of the Computer, the Internet and Management, Vol. 19, No. SP1.
3. Dr. Sunil Bhutada,Preeti Bhutada.Applications of Artificial Intelligence in Cyber security International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 4, April 2018 All Rights Reserved © 2018 IJERCSE 214
4. Nikita Rana, Shivani Dhar,Priyanka Jagdale, Nikhil Javalkar. Implementation of An Expert System for the Enhancement of E-Commerce Security International Journal of Advances in Science Engineering and Technology, ISSN: 2321-9009 Volume- 2, Issue-3, July-2014
5. M.M. Gamal, B. Hasan, and A.F. Hegazy, “A Security Analysis Framework Powered by an Expert System,” International Journal of Computer Science and Security (IJCSS), Vol. 4, no. 6, pp. 505-527, Feb. 2011.
6. K. Goztepe, “Designing a Fuzzy Rule Based Expert System for Cyber Security,” International Journal of Information Security Science, vol.1, no.1, 2012.
7. D. Welch, “Wireless Security Threat Taxonomy,”InformationAssurance Workshop. IEEE Systems, Man and Cybernetics Society, pp 76-83, June 2003.
8. Vidushi Sharma, Sachin Rai, Anurag Dev” A Comprehensive Study of Artificial Neural Networks” International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 10, October 2012.
9. Shaiqua Jabeen, Shobhana D. Patil, Shubhangi V. Bhosale, Bharati M. Chaudhari, Prafulla S. Patil” A Study on Basics of Neural Network” International Journal of Innovative Research in Computer and Communication Engineering Vol. 5, Issue 4, April 2017.
10. Devikrishna K S, Ramakrishna B B “An Artificial Neural Network based Intrusion Detection System and Classification of Attacks ”International Journal of Engineering Research and Applications (IJERA) Vol. 3, Issue 4, Jul-Aug 2013, pp.1959- 1964.