IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⋇ Impact Factor 7.918 ⋇ Vol. 12, Issue 1, January 2023

DOI: 10.17148/IJARCCE.2023.12137

A Review on Recent Tools in Cyber Security

Sathvika Ontela[1], Sanjana Nuguri[2], E. Soumya[3]

B. Tech, Student, Department of CSE, St. Martins Engineering College, Hyderabad, India[1,2]

Asst. Professor, Department of CSE, St. Martins Engineering College, Hyderabad, India[3]

Abstract: Artificial Intelligence and machine learning are the emerging technologies in the world in every fields. Mainly emerging in the security fields. These technologies are promising to improve convivence and comfort of the user by securing the data and resolving the problems like cyber-attacks, communication security, big data security, cloud based, social media, finance, IOT and weapon detection. Many companies promote their product using social media and e-commerce platform. These platforms provide more opportunities for companies to attract customers. Trusting these platforms many customers started purchasing products from them. At that same instant many fake accounts have been created by replicating the organization names. By making online payments through these sites the customers are getting charged for the product they never placed. In this paper, discussion is classified into two parts. First part describes about the security using the AI-ML technologies and algorithms and also a review of AL-ML based security systems and methods, in the second part it describes about online fraud detection by training classification model using ML technology.

Keywords: Cyber-attacks, big data security, IOT, Cloud based, AI-ML

I. INTRODUCTION

Security a form of protection or resilience against potential harm by restricting an individual‘s freedom. Mostly refer as protection from hostile forces. Security has an ancient Egypt history where the main purpose of security is “securing the data”.

Security has a lot of divisions according to the realm. It can be the IT realm, physical realm, political realm, monetary realm. Security is highly preferred by any realm because it has the confidently, record integrity, non-repudiation, authentication.

Security in IT realms are usual in these days. There is an increase rate of cybercrimes. These crimes usually accompany the devices which is caused by the outsiders or the careless of the device users. Artificial intelligence has taken a lot of development in the stage to improve cyber security. It is widely used in almost all the industries including smart manufacturing, medical care and home furnishing. It has few technical standards such as common intelligence, privacy intact, interconnection between devices, and network security.

The development of technology in computer is promoting the development of artificial intelligence. Artificial intelligence is a duplication of human brain. It helps increasing the productivity also simplifies the operations. The problems faced by the computer technology is solved and hence security is maintained.

Tools that are used to protect an organization data such as firewalls, IPS, anti-viruses, antimalware will not support some of the activities so, those can be done using artificial intelligence

The technologies used by the artificial intelligence in the cybersecurity are the Supervised learning, semi supervised learning, unsupervised learning, reinforcement learning, neural network, In-depth learning.

Abnormal unpredictable items or events are identified using anomaly or weapons detection. Various categories of objects are recognized by feature extraction and learning algorithms or models. Based on application various suitable detection algorithms are chosen for gun detection using deep learning.to extract useful information for humans to determine spams.

II. METHODOLOGY

Social networking site is to associate people and organizations along with developing business opportunities for companies and firm. Social media has introduced the Significant changes the way people communicate. Social networking sites bring out the specific function related to privacy and security of the user. Social e commerce site can be used for advertisements and provide a better platform for company to apply customers for different business opportunities. The e commerce platform allows easy admission of shoppers to perform a self-service purchase. It offers real time transactions across a wide geographical region. E commerce is exhibiting a sky rocketing growth both in popularity and the amount of money generated from this platform.

Online payment fraud can happen with anyone using any payment system. Especially while making payments using a credit card that is why detecting online payments fraud is very important for credit card companies to ensure that the customers are not getting charged for the products and series they never played.

FRAUD DETECTION

Detection and prevention from fraudsters from invading one individual's personal property is fraud detection. There are many forms of frauds, every business model gets adapt to fraud. Common types of frauds

- Stolen credit card purchase
- Account takeover
- Fake account
- Affiliate fraud
- Bonus abuse

Fraud detection can be done based on data analytic techniques. Fraud detection techniques are broadly classified into two types 1) Statistical data analysis technique 2) artificial intelligence techniques.

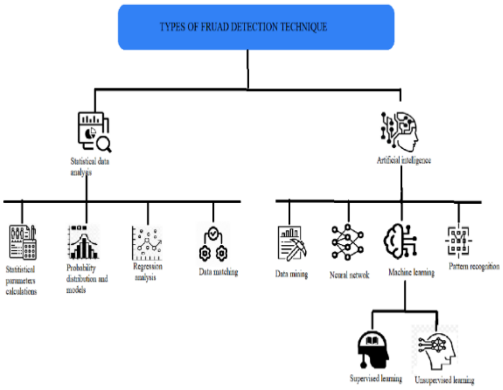

Fig:1 Types of fraud detection

With the growth of e-commerce website many companies and customers relay on online services, with increase in number of transactions it led to increase in credit card frauds. The design of fraud detection should reduce the losses incurred in money of customers and companies. Many research have been done on credit card fraud detections, but some of the datasets contain the problem of unbalancing data. A good fraud detection system should determine fraud transactions accurately in real time applications. Anomaly and misuse detections are the two groups divided from fraud detection. Anomaly detection use normal transactions to be trained and by using technique it determines fraud transaction. Misuse fraud detection system uses labelled transactions or fraud transactions to train the model then it determines the fraud.

III. LITERATURE SURVEY

Artificial intelligence has been used in different fields, also in computer networks using this it can have many advantages to provide people with convenience in life and production and it also helps in providing security and network management [1]

As the internet is expanding many communication traffic attacks are happening which can lead to serious impact, as wide range of application have developed using artificial intelligence it can be used for communication security by finding fault characteristics and faults points. The paper gives complete examination of its development standardization and application by mentioning Supervised learning, Unsupervised learning, Semi Supervised learning, Neural network, Reinforcement learning, In-depth learning [2].

The paper emphasizes study of artificial neural technology, data mining technology, security management, problem solving technology to create a safe computer network environment using artificial intelligence under the background of big data. Through this application the hazard in the system can be identify in time, unstable elements can be outline to prevent their intrusion into the system and influencing information security [3].

The paper proposed new objective to use AI in dependable services, the idea concentrated on user behaviour more than event-based detection pointing out deep learning, rule-based methodology, long term behaviour detection and introduced a simple equation to explain the rating of the malicious level. In the end, the proposed method can rapidly demce the suspicious target to forensic [4]. This paper explained the feature of the internet of transportation system with respect to AVs also the security and privacy concern and deliberated on how AI and security maybe integrated. Also includes virtual network monitor, physics-based anomaly detection algorithm, CUSUM [5]. This paper describes advantages of social media and the application of machine learning techniques for social media. Machine learning techniques, access control model's authentication techniques to detect fake news and malicious software. Finally discussed adversarial machine, the inference and privacy problem for the integration of AI and cyber security for social media system [6]. The paper proposed an AI based SOAR system in which the data from different sources like firewalls, IDS etc is gathered with separate event describing a deep learning detection method. This includes 1.AI technique based on artificial neural network Deep learning-based technique, FCNN, CNN, LSTN neural network methods, machine learning algorithms, AI based SIEM, SOAR [7]. This article depicts the idea of artificial intelligence technology, the problems faced by computer networks, additional analysis, the benefits of artificial intelligence and unavoidable of application in network technology, then examines for the application of artificial intelligence in computer network technology using Intelligence firewalls, Anti-spam, intrusion Detection, AI agent technology, Intelligent network management technology [8]. This article describes the impact of AI on financial innovations on this basis proposed a measure for innovations and development of bank financial science and technology. By using Voice recognition technology, big data algorithm, Artificial Intelligence methods. The problem of computer information security management in bank financial innovation in the period of artificial intelligence. [9]. This article executes automatic gun or weapon detection using Deep learning, Frame differencing algorithm, SSD or fast RCNN machine learning models, SSD-single shot detection, RNCC- region convolutional neural network. There algorithms implemented with good veracity, but the application in real scenarios can be based on arrangement between speed and accuracy. SSD-accuracy 73.8% RCNN-accuracy 84.6%. [10]

Different examines have been performed to explore the feasibility of detection of web-based attacks by machine learning techniques. In this research identification and addressing the root cause of false positive and false negative results have been done. This includes by using CSIC 2010, HTTP Data set, J48-decision tree (94.5% accuracy), OneR (one rule)-rule system Naive Bayes-Bayesian ML models [11]. Access to the data which is protected from the network susceptibility, malicious users or unauthorized users through the network is a big task. The novel framework is used for producing high security, by using the mathematical approach for solving these problems efficiently. This also includes Precision and prediction, Novel numerical approach with Machine Learning Technology, Nash equilibrium [12].

The paper addressed crucial security hazards that present at IOT layers and analysis machine learning based IOT security system with concentration on supervised learning. Machine learning based security methods like Support vector machine Random Forest, Decision tree, Artificial Neural Network for various IOT applications.>Accuracy:99.5%,>Root means square error: 0.0171, >Decision Tree accuracy:99.4%, >Detection Accuracy:99%. [13].

As today's informational environment it's an important task for the prevention of DDoS attack. The theoretical part of the classical machine learning algorithms is considered here. The requirements of functional and non-functional were identified. The traffic classification system appearing as a window application developed. The machine learning algorithms that are used are K-NN, Naive Bayes, SVM, Ridge/Lasso, Decision Tree and K-Means accuracy 46.6% to 99.8%. Accuracy ranged between 46.69% to 99.81% based on the algorithm use [14].

IV. PROPOSED METHODOLOGY

The Significant security issue in credit card application is data breach occurs whenever unauthorised access to sensitive data. During the payment process using credit card the private data is at risk when it is in at rest, in transits and in use. For example: when card holder's data is in use, which is in readable state and used for transaction operations. Unauthorized been known to hack into the memory of computer while acquirer's computer is reading card data, in order to steal sensitive data. Data encryption is complex and often way to protect card holder's data but there is a new way for data protection beyond encryption called tokenization. So, in tokenization process it generates random tokens to access credit card information securely where the token doesn't contain any sensitive data by acting like maps explaining where the sensitive data is within their own system. This can be generated through mathematical algorithms. Byte -pair encoding algorithm in NLP is used to generate token by splitting the data. Tokens can be unlocked after the transaction process completed, outside the system there is no meaning or value even hackers cannot access the sensitive data while processing the transactions, has data been tokenized. Tokenization provides transaction safety by reducing chances of frauds from sharing card details.

DATA COLLECTION

We need to collect the data which contain online payment transaction and different transaction modes, so we can detect which type of transaction lead to fraud. The data set that we have collected should consists of historical and fraudulent transaction to train the model for detecting credit card transactions.

For this application the data set is collected from Kaggle.[15]

TYPES OF TRANSACTIONS

Based on exchange of cash transactions are classified into external and interval. In the data set(paysim) that we have collected may consists of transaction types

1) Cash out
2) Payment
3) Cash in
4) Transfer
5) Debit

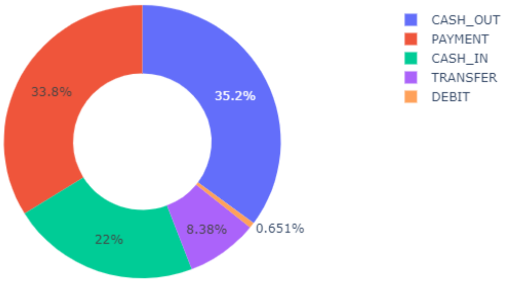

Fig:2 Distribution of transaction type for collected data

CORELATION

Corelation is statistical technique which determines the relation of one variable which changes of another variable. It gives an idea of degree of relationship between two variables. These variables can be input data features to forecast out target value. In credit card fraud detection application, we need to find the core relation between features of data with fraud column of the data set. Train a classification model (The model that classifies or draw a conclusion from input values given for training. It will predict class labels for new input data. It helps in predicting class labels for new input data.) to classify fraudulent and non-fraudulent transaction.

To classify whether the transaction is fraudulent or non-fraudulent. We need to fed a transaction to classification model that we trained

TRANING MODEL

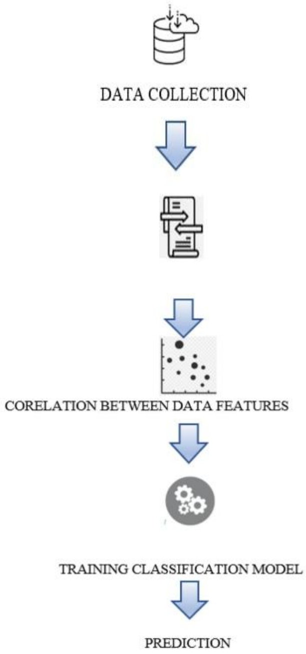
DATA COLLECTION
CORELATION BETWEEN DATA FEATURES
TRAINING CLASSIFICATION MODEL
PREDICTION

Fig:3 Steps for data training

DOI: 10.17148/IJARCCE.2023.12137

BENEFIT OF MACHINE LEARNING IN FRAUD DETECTION

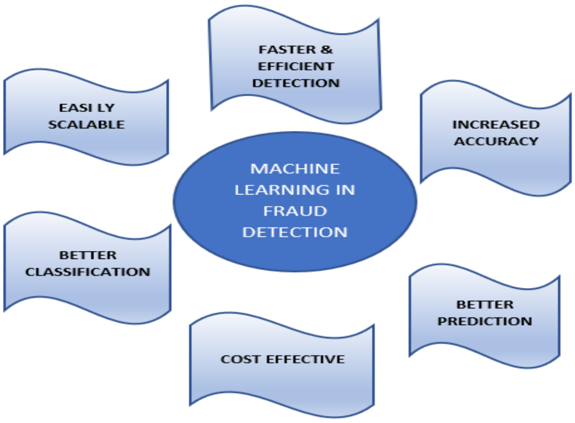

Fig 4: Benefits of Fraud Detection

CONCLUSION

In this survey, we have dispensed different security hazards that are existing in different fields of computer system. After a thorough study on different analysis and solutions on security attacks using AI and machine learning technology. Mainly focusing on Supervised learning, unsupervised learning, semi supervised learning and their sub divisions. These have the potential to improve the security for various computer networks. In fraud detection, for the chosen data set(paysim) we trained a classification model using ML technique for detecting fraud transactions. The model trained using ML is self-learning which enables to adapt new features, it is easy to deploy and also can modify the code to work with any data set. ML model provides better classification and prediction with faster and efficient detection and increases the accuracy in detecting fraudulent transactions.

REFERENCES

[1] Xian Shang, changong Zhao "Research on Application of Artificial intelligence in the computer network technology "2020 5th international conference on mechanical, control and computer engineering (ICMCCE)

[2] Sun Wenhui, Wang kegin, zhu Aichun "The Development of Artificial intelligence technology and its Application in communication security "2020 international conference on computer engineering and applications (ICCEA)

[3] Bao Julian "Research on the technology of Artificial intelligence in computer network under the background of big data "2020 international conference on computer communication and network security (CCNS)

[4] Tsung-yu ho, Wei-An Chen, chiung -Ying huang "The burden of Artificial intelligence on internal security detection" 2020 IEEE 17th international conference on smart communities: improving quality of life using ICT, IOT and AI (HOMET)

[5] Bhavani Thuraisingham "Cybersecurity and Artificial Intelligence for cloud-based internet of transportation system "2020 7th IEEE international conference on Cybersecurity and cloud computing (CS cloud)/2020 6th IEEE international conference on edge computing and scalable cloud (EdgeCom)

[6] Bhavani Thuraisingham "The Role of Artificial intelligence and Cybersecurity for social media "2020 IEEE international parallel and distributed processing symposium workshops (IPDPSW)

[7] Rahul vast, Sruthi swath, Aishwarya Thorbole, Vishal Badgujar "Artificial Intelligence security orchestration Automation and Response system "2021 6th international conference for convergence in technology (12CT) pune, India April 02-04-21

[8] Yanjie li "The Application Analysis of Artificial intelligence in computer Network Technology "2021 IEEE Asia-Pacific conference on Image processing, electronics and computer (IPEC)

[9] Xiaoyi hu*, Ke wang" Bank financial innovation and computer information security management based on Artificial Intelligence "2020 2nd international conference on machine learning, big data and business intelligence (MLBDBI)

[10] Harsh Jain, Aditya Vikram, Mohana, Ankit Kashyap, Aayush Jain "weapon detection using Artificial intelligence and deep learning for security Applications "proceedings of the international conference on electronics on sustainable communication systems. (ICESC 2020) IEEE Xplore part Number-CFP20V66-ART; ISBN-978-1-7281-4107-4

[11] Sushanth Sharma, Pavol zavarsky, Sergey Butakov "Machine Learning based intrusion Detection System for web-Based Attacks "2020 IEEE 6th international conference on big data security on cloud (big data security), IEEE international conference on high performance and smart computing, (HPSC)and IEEE international conference on intelligent data and security (IDS)

DOI: 10.17148/IJARCCE.2023.12137

[12] T.P.Anithaashri,G.Ravichandran” Security enhancement for the Network Amalgamation using Machine Learning Algorithm “proceedings on international conference on smart electronics and communication (ICOSEC 2020) IEEE explore part number:CFP20V90-ART;ISBN:978-1-7281-5461-9

[13] Shikha Malik, Ruchi Chauhan “securing the internet of things using Machine Learning: A Review” 2020 IEEE international conference on convergence to digital world-Quo Vadis (ICCDW 2020)

[14] Evgenii Nazarenko, Vitali Varkentin, Aleksey minvaleev “Applications for traffic Classification using Machine Learning Algorithms “2020 international conference on quality management, transport and information security, information technologies (IT &amp; QM&amp; IS)978-1-7281-8179-0/20/$31.00 2020 IEEE