Forensic accounting and Cybersecurity examine their interrelation in the detection and Prevention of financial fraud

Dr.Osama Matar

Abstract: Due to the increase in the number of financial crimes and the increase in the number of cases related to this type of crimes in the courts, and because the task falls on the shoulders of a judicial accountant, the classical methods no longer work because of the complexity of cases and the increase in their number, and because the development of technology has contributed to the increase in the number of these crimes, also contributed with techniques through artificial intelligence in data analysis and easy access to solving these crimes, and this study aims to identify the effectiveness of machine learning in criminal accounting and its ability to facilitate the work of judicial accountants vıa Fraud detection is one of the main applications of artificial intelligence and machine learning in forensic accounting. By analyzing large data sets, machine learning algorithms can identify patterns and anomalies that may indicate fraudulent activity. These algorithms can also learn from previous cases and improve their accuracy over time ,Machine learning algorithms can identify irregularities and inconsistencies that may indicate financial crimes such as money laundering, embezzlement and tax fraud and is used in predictive analytics, allowing forensic accountants to anticipate possible financial crimes before they occur

1. Introduction

The dizzying speed of globalization is making itself felt intensely in financial markets, as in every field. Today, as a result of globalization, the boundaries between regional and local financial markets have been Decoupled, and full financial integration between different markets is being achieved. Decoupled financial integration between regional and local financial markets is being achieved. “Financial integration”, which is expressed as the close interaction of a local financial market with markets operating in other geographies, covers the process of harmonization of financial practices and regulations belonging to different countries (Erkan, 2005).

The fact that financial integration serves the purpose of “creating a global market” by Decoupling the boundaries between local and regional markets is considered one of the positive effects of globalization. However, on the other hand, the global economy can leave companies facing a wide range of risks. The impact of an accounting fraud or fraud carried out by any company in any geography can be felt even in another company on the other side of the world today. In the same way, information and communication technologies, which are developing extremely rapidly with globalization and are being used extensively, are causing the emergence of new risks that companies have not experienced in the past anymore.

In addition, especially 20. accounting scandals and corporate frauds that have occurred since the century prove how open companies are actually to accounting fraud and fraud. Companies that remain vulnerable to accounting fraud are taking several measures to reduce the potential losses they will face. As a result of the inability of classical methods aimed at preventing accounting fraud to respond adequately to today's conditions, technological methods such as machine learning are used to prevent economic crimes. (Moore ve Mills, 2014)

Groups that remain prone to accounting fraud are taking several measures to reduce the potential losses they may face. Due to the inability of classical strategies aimed at stopping accounting fraud to reply competently to cutting-edge situations, technological methods along with gadgets getting to know are used to save you from economic crimes. Artificial Intelligence (AI) and device getting to know (ML) have been around considering a long term however it's far now that we have sufficient computational strength to effectively develop sturdy artificial neural networks (ANN) in a realistic time body with the assistance of robust hardware and software help. Businesses like Google, Amazon, Samsung, and so forth. Are heavily investing in AI technologies and funding the research. Google CEO Sundar Pichai introduced the business enterprise's vision to be "AIFirst" at Google I/O 2017 and quoted "It's all about a transition, from looking and organizing the world's statistics to AI and system learning.

Google also unveiled the "TensorFlow studies Cloud" application to offer researchers with get entry to a thousand cloud TPUs (Tensor Processing units) free with a condition to open supply their code and studies because AI is becoming extensively to be had by more and more human beings, the potential of the generation for use for malicious purposes additionally increases extensively. To counter this and be prepared for forensic challenges regarding crimes devoted to AI or ML, forensic evaluation and analysis of the generation are important. This paper demonstrates the implementation of a device gaining knowledge of open supply software "DeepQA" and forensic analysis of the same even as this system turned into in schooling and checking outmodes.

Artificial Intelligence (AI) and machine learning (ML) have revolutionized the field of Forensic Accounting by providing sophisticated and efficient methods for detecting, preventing, and investigating financial fraud. Forensic accounting involves the use of accounting, auditing, and investigative skills to identify and investigate financial crimes, such as money laundering, embezzlement, and securities fraud.

Machine learning is a subset of AI that involves the use of algorithms and statistical models to enable computers to learn from data, without being explicitly programmed. Machine learning algorithms can analyze large volumes of financial data to identify patterns and anomalies, which can help forensic accountants to detect fraud more efficiently and accurately One of the key advantages of using machine learning in forensic accounting is that it can automate many time-consuming tasks, such as data analysis and pattern recognition. This allows forensic accountants to focus on more complex tasks, such as investigating suspicious transactions and interviewing suspects. (Alma ,2019:90)

1.1 Research Problem

Due to the high rate of financial crimes, this was due to the advanced technologies used by the perpetrators of these crimes, such as social engineering, hacking, malware, credential stuffing, skimming, and open source .. Because of the difficulty of determining the perpetrators of these crimes by classical methods, the problem of the study lies in knowing What are the ways in which artificial intelligence and its technologies can contribute to reducing this type of crime and how does it make it easier for forensic accountants to do forensic accounting

1.2 Study questions

1- What are some specific techniques within artificial intelligence (machine learning) that can be used in forensic accounting, and how do they work?

2- What are some real-world examples of how artificial intelligence (machine learning) has been used in forensic accounting to detect financial crimes or analyze financial data?

3- What are some potential limitations or risks associated with using artificial intelligence (machine learning) in forensic accounting, and how can these be mitigated?

4- How do current regulations and ethical considerations impact the use of artificial intelligence (machine learning) in forensic accounting?

5- What are some potential future directions for research and development in the field of artificial intelligence (machine learning) in forensic accounting?

2. Background and related work

The use of machine learning in forensic accounting is gaining popularity as technology continues to evolve. Machine learning involves the use of algorithms and statistical models to enable computers to learn from data, and make predictions or decisions without being explicitly programmed. It has many applications in forensic accounting, including fraud detection, financial statement analysis, risk assessment, and predictive analytics.

One of the major contributions of technology to reducing financial crimes is the ability to process large volumes of data in real time. This has enabled forensic accountants to identify anomalies and patterns that would have otherwise been missed using traditional methods. Machine learning algorithms can identify hidden relationships and correlations in financial data that can be used to detect fraudulent activities, such as money laundering and embezzlement.

Another way that technology has contributed to reducing financial crimes is through the use of artificial intelligence (AI) chatbots. These chatbots can be used to identify potential fraudulent activities and notify forensic accountants in real time. AI-powered chatbots can also assist in identifying and mitigating cyber threats, which have become a significant challenge for organizations in recent years.

In addition, technology has made it easier to investigate financial crimes across borders. The use of cloud computing and advanced analytics tools has made it possible to access and analyze data from anywhere in the world. This has enabled forensic accountants to collaborate more effectively with their colleagues in other countries and to track financial transactions across multiple jurisdictions.

2.1 The concept of ACCOUNTING FRAUDS

Accounting scandals carried out by industry giants such as BCCI (The Bank of Creditand Commerce International) in the UK in 1991, Enron in the USA in 2001, WorldCom in the USA again in 2002, Parmalat in Italy in 2003 caused great losses to both employees and investors and the entire society as a result of fraudulent financial transactions. Likewise, the accounting scandals carried out by Toshiba, Volkswagen and General Electric in recent years show that the fraudulent transactions of these multinational companies are felt on a global scale and, more importantly, cause great material and moral losses in the markets. The accounting scandals caused by these companies as a result of fraudulent accounting transactions also undermine the goal of achieving social benefits and undermine confidence in the markets.

In addition to their economic costs, accounting fraud, fraud and abuse can cause critical damages (both mental and physical) to their victims and the consequences can be much more serious and lead to the formation of a climate of insecurity in society (Moore and Mills, 1990). As the violence of these actions increases, the situation may cause more serious consequences, such as experiencing economic trauma in society.

Since these cheats, frauds and abuses, which can also be referred to as economic crimes, are inevitable and their consequences are very expensive for both companies and investors, as well as for the entire society, the subject has become an important research trend, especially in the fields of accounting, corporate governance, law and forensic sciences. The victims of economic crimes actually know that the rapid (sudden) damage caused by the crime has consequences far beyond its material dimension. The emotional collapse caused by these crimes shows that in addition to the material damage expressed in figures, more different harms are endured. The most important of these damages is the destruction of trust, which is also vital for organizations (Friedrichs, 2010; Gambetta, 1988) and therefore the social trust climate (Dearden, 2016:88). Trust should be evaluated both in terms of economic crimes and as an antecedent phenomenon of legal (legitimate) commercial activities (Cressey, 1980). For this reason, these crimes, the consequences of which create costs for all segments of society, need to be considered in detail.

One of the most basic motivations underlying the organizations of companies is the company's goal of “profit generation and maximization of this profit”. But on the other hand, companies must also take into account the public interest in achieving these goals. For this reason, companies need to be prepared against accounting fraud, fraud and misconduct that will be carried out by both managers in middle and upper management and lower-level employees in order to provide public benefit. Companies are obliged to take the necessary measures to prevent these potentially criminal acts in question and to deter potential criminals from committing these criminal acts.

The costs that companies will incur in order to prevent potential crimes are usually equal to or less than the actual costs that they may face in the event of the occurrence of this crime. In other words, the crime itself is more costly than its deterrence. Therefore, companies should be careful against accounting tricks, fraud and abuses that will be carried out by their employees. For this purpose, companies should establish control mechanisms in order to keep the accounting practices they practice under supervision and supervision and take steps to prevent possible accounting irregularities before they are revealed.

2.2 PREVENTION OF ACCOUNTING FRAUD AND ITS THEORETICAL FOUNDATIONS

Although there are many theories aimed at preventing crime in the crime literature, the perspectives of these theories on the phenomenon of crime differ among themselves. Dec. Some of these theories about crime prevention take the criminal act itself as the point of departure; some theories focus on the criminal individual or the factors that cause crime formation rather than the criminal event itself. One of the theories for crime prevention today is the situational crime prevention approach. Felson (1996) explains the situational crime prevention approach as “methods used to prevent crime by destroying the opportunities that enable crime to be committed ”.According to Clarke (1997), crime prevention measures should be “evaluated as a scientific discipline to function more effectively and efficiently and to cover the whole society”, and thus the situational crime prevention approach is revealed (Malkoc, 2014:3).

The situational crime prevention approach argues that preventing crime by reducing crime opportunities is possible through efforts such as measures to be taken, administrative decisions, and environmental regulations. At the heart of the situational crime prevention approach is the goal of reducing crime opportunities. To fulfill this purpose, the approach states that the risks of being caught by individuals who commit crimes should be increased and the benefits to be provided from crime should be reduced (Dolm, 2009). Within the framework of this approach, environmental factors that are effective in exposing crime are determined and it is argued that criminal incidents can be prevented by limiting or eliminating these factors (beker, 2009:84). The most basic starting point of the situational crime prevention approach is the purpose of preventing the absolute situations, opportunities, risks, and opportunities that prepare the ground for the occurrence of crime and reducing or completely preventing crime before it even occurs (Clarke, 1997).

The situational crime prevention approach finds its application in many developed countries, especially in the United Kingdom, the Netherlands, and Sweden. The approach was first included in the criminology literature in 1997 by Clarke and Homel, who are the fathers of the idea. Clarke and Homel mentioned crime preventive measures that serve to make the commission of a crime difficult or to restrict the time of committing a crime within the framework of the situational crime prevention approach (beker, 2009:86). There is an assumption that individuals who can be classified as potential criminals within the framework of the situational crime prevention approach decide to commit a crime based on their personal preferences, and during making this decision, they take into account the possible costs caused by criminal actions and the benefits they will receive from crime. Within this framework, it is expected that the benefit that individuals who may be classified as potential criminals will receive if they commit crimes will be greater than the cost that they will bear.

Clarke (1997) systematized the measures aimed at crime prevention and regularly taken by both individuals and companies and included them in the literature as a situational crime approach. The situational crime prevention approach is not concerned with the elimination of crime through the development/improvement of the social order or social institutions shaped by the rules, norms, and values that dominate society as a whole. In the same way, the situational crime prevention approach puts the issue of catching the perpetrator of the crime and subjecting him to the criminal sanction required by the crime in second place. The focus of this approach is to ensure that the criminal act is made less attractive for individuals with criminal potential (Clarke, 1997). According to this approach, the individual who will make the decision to commit a crime avoids committing a crime within the framework of his own free will. From the point of view of companies, the situational crime prevention approach serves the purpose of keeping internal and external stakeholders of companies away from committing crimes.

According to the situational crime prevention approach, which expresses the need to make various administrative and environmental regulations to minimize the possibility of crime occurrence, to take some measures within companies to prevent economic crimes they have to. These measures require companies to use proactive methods against economic crimes that are extremely likely to occur. One of the most proactive mechanisms that companies can benefit from is a well-functioning internal audit system and an independent audit process.

The basis for the commission of economic crimes within the structure of companies is the internal audit systems that do not work regularly. Although it may be encountered by companies that have internal audit systems in their structure, these systems are not taken into account by their employees very much. The mentioned situation has a great impact on the occurrence of economic crimes in companies. In addition, although companies have a strong internal audit system, company employees can circumvent these internal audit systems through confidential collaborations they have realized (KPMG, 2013:23).

On the other hand, companies can create risk management systems to prevent potential economic crimes that may occur within their structures. However, to talk about an efficient and effective risk management system, companies must be adapted to the characteristic cultural characteristics of the country in which they operate. Another way in which economic crimes can be prevented within the framework of the situational crime prevention approach is the establishment of in-house notification lines. In addition to preventing situations that prepare the ground for crime, which is one of the actions taken to prevent economic crimes, educating and raising awareness of employees about these crimes is an obligation for the company. The fact that economic crimes can cause enormous damages and the costs they cause are quite high shows quite clearly that awareness at the company level alone is not enough. In other words, awareness should be raised against these crimes at the macro level as well as at the community level. For this very reason, it is necessary that the commitment of the individuals who make up society to ethical values and trust in the law should be complete. The way to ensure full confidence in the law is through the establishment of an effective legal system that punishes the criminal and protects the victim of crime. The punishments prescribed by law should ensure that potential offenders are deterred from the criminal act and should be of a speed and severity that will satisfy the victi.

Increasing the severity of sanctions in deterring economic crimes does not give the expected effect in preventing criminal acts and is not enough in itself. Only an increase in the severity of the punishment required by the crime is not a complete deterrent to committing crimes; in addition, in a manner commensurate with the crime, it must be known that the criminal punishment required by the crime will be applied in a specific form and the final punishment must be carried out on time. Here are some steps that the judiciary should take to prevent economic crimes (kaya, 2013: 139):

Preference for the most honest forensic accountants and organization of the work environment in order to prevent crime

- Provide special support programs in order to provide support to accounting personnel, establish an internal audit system to ensure the company's internal audit, inform internal and external stakeholders about the company's policy, supervise the performance of the company's employees, through the establishment of internal company notification lines, to ensure that these lines are working during a possible crime to ensure that employees are aware that they will be punished if they commit crimes.

Although these above methods are still valid today, they cannot maintain their former popularity with the transition from the classical to the modern management approach. Nowadays, with the impact of globalization and rapidly developing technology, it has become very easy to carry out fraud and accounting fraud; the costs of these accounting crimes are heavier than ever. In addition, as a result of the expansion of markets and an increase in trade volumes, the Prevention of accounting crimes is becoming more and more important. For this reason, there was an obligation on companies to take precautions and beware of these irregularities. Companies are taking advantage of the new opportunities offered by very rapidly developing information and communication technologies in detecting and even preventing fraud and accounting fraud. In addition to the classic methods of detecting irregularities such as reports prepared as a result of the audit, opinions of the auditor and senior managers, interviews with employees (Essen, 2016:95), technologies are now being used that allow making forecasts and forecasts to determine the company's position against accounting irregularities in the light of historical and current data (Atan, 2016: 140). One of the most important of these technologies, which includes many methods such as data mining, predictive methods, deep learning, artificial intelligence, is machine learning .

2.3. Machine learning

Artificial intelligence is basically an artificial operating system; this operating system is expected to display a number of human-specific features and behaviors. It is expected that" various complex cognitive activities such as movement, speaking, sensing, learning, thinking, reasoning, finding solutions to problems, communication, voice detection, decision-making and making conclusions " that only humans can do will be carried out by artificial intelligence. From this artificial OS in question, they are expected to embody their thoughts in an expression/reaction, just like humans, expressing them through physical reactions (Adam, 2020). The basis of the concept of artificial intelligence, which can be expressed as a whole of software and hardware systems, is "the purpose of ensuring the ability of computers to think like humans" (Tagiyev, 2020). Artificial intelligence has already been developed to take human capabilities and contributions to higher levels. Artificial intelligence, working within the framework of the principle of taking human intelligence as an example or imitating it, can constantly improve itself (Oracle, 2020).

Artificial intelligence, a branch of computer programming, analyzes people's thinking, their abilities to learn and think in detail and aims to create artificial instructions by taking these abilities as an example for itself (Aksu, 2017).

In order to understand artificial intelligence more clearly, it is necessary to focus on machine learning, which can be expressed as a sub-branch of it. Machine learning can be interpreted as algorithms that allow machines to reach logical and rational results according to the available data obtained (Tagiyev, 2020). According to another definition, machine learning refers to all computer algorithms that perform modeling with data on the current problem in order to solve a problem (Orhan, 2012). According to Akai (2018), machine learning is a sub-branch of artificial intelligence that makes conclusions based on current data and allows making predictions about the future, in other words, about knowledge. Akai mentions that machine learning uses different mathematical and statistical methods while creating these estimates. Machine learning, which allows making future-oriented predictions based on the conclusions obtained, realizes these predictions by modeling them using a computer.

In improving the application of Forensic Accounting, machine learning allows the court to make future-oriented predictions by decoding and processing the structure of each data contained in the data set. In this direction, it is about making data more valuable by processing future forecasts and making them more efficient.

Through machine learning, it is possible to reveal how huge amounts of data are processed by processing information obtained through a computer, and how decisions can be made about data just as people did. Based on machine learning, it is the sum of a number of methods and techniques that allow computers to identify certain patterns and trends and make predictions based on these patterns and trends (Ravelin, 2020).

Machine learning analyzes huge amounts of data effectively and efficiently in real time and creates risk scores . While machine learning makes predictions about the patterns of behavior that forensic accounting will show in the future based on historical data while carrying out these analyzes, it realizes this prediction by identifying the digital fingerprints of criminals(fedzai, 2020).

Machine learning is also leading forensic accountants to gain a cost advantage by being able to do things that people can do in a very long time in very short periods of time. Data processing, a very cumbersome task for humans in terms of time and money, can be done by computers in a very short time and at very low costs thanks to machine learning. In the same way, machine learning can achieve more efficient results than auditors in detecting cunningly conducted frauds, criminal tendencies and counter-intuitive behavior patterns that fraud auditors may not immediately notice at first glance.

The fact that machine learning is much faster than traditional fraud detection methods and makes it possible to work with larger data sets allowed it to find a wide range of applications in the field of accounting. Situations where there is no fraud and the good situations that fraud involves as references to bad situations through machine learning, companies can easily identify good and bad situations from their own point of view. In addition, machine learning makes it possible to more decently identify the differences and similarities between good and bad situations. Thus, predicting whether the transactions that companies will make in the future contain fraud can be done in a healthy way through machine learning.

Today, with the impact of globalization, accounting irregularities can be realized in many different ways. In addition, due to the highly dynamic structures of fraud patterns, it may be possible to constantly create new fraud patterns. It is very difficult for forensic accountants to keep up with these new fraud patterns that are all occurring is a situation where the mentioned frauds are mostly targeting the weakest points of the companies. In addition, the fact that efforts to prevent fraud are often very time-consuming and expensive makes companies more careful and sensitive about this issue. For these reasons, companies often use machine learning to protect their companies from fraud. On the other hand, it may be possible for a company to identify suspicious customers through machine learning before the criminal act is detected or the criminal act is detected. The steps of the machine learning process are as follows:

The first step in the machine learning process is data entry. The more data that will be evaluated in machine learning in identifying accounting fraud, the more accurate the results will be achieved. More clearly, more data in fraud detection is the key to more correct results. It is possible to talk about two basic types of learning in machine learning, in other words, two types of machine learning algorithms: supervised/supervised learning (supervised) and unsupervised learning in supervised learning, tagged observations form the basis of the learning process. In this type of learning, there are educational data that make up the majority of the data, and the algorithm learning process is created from this educational data.

Subsequently, this learning process is controlled by test data. For this reason, this type of learning is expressed as supervised learning and supervised/ machine learning focuses mainly on problems related to prediction and inference. In this type of machine learning, a model is being developed that makes it possible to make predictions based on the available evidence in cases where uncertainty prevails. In this method, first of all, by working with a known data set, the expected outputs (known responses) related to the data are obtained. In the next step, he aims to arrive at reasonable estimates with the new data set. For this reason, the first step of supervised/supervised machine learning is about teaching the model a known dataset. In cases where there is an estimated output related to known data, supervised/supervised machine learning is used (device, 2020).

Supervised/supervised machine learning is evaluated under two subheadings as "regression" used for quantitative variables and "classification" used for qualitative variables. While "regression is a type of supervised/supervised learning used to make predictions and conclusions about quantitative variables"; "classification can be expressed as a type of supervised learning related to the allocation of observations to qualitative categories for modeling and forecasting qualitative variables" (Akai, 2018). One of the two basic learning types of machine learning is unsupervised/unsupervised learning. Unsupervised/unsupervised learning in its simplest form can be expressed as the"learning process from unnamed observations". In this type of learning, the purpose is to discover and expose groups within the data set that do not have classroom information or are not provided. Unsupervised learning can be interpreted more clearly as the process of discovering invisible structures and forms of an algorithm on its own (Adam, 2017).

In this type of learning, although there is no need to revise the model; The model should be able to work on its own without interference. Unsupervised learning algorithms that work more comprehensively compared to supervised learning, learn that they perform their work through data. In other words, the system is not taught in these algorithms; it learns on its thanks to the data. In addition, using this method, can detect various unknown patterns shown by the data and reveal criteria that can be considered useful for classification (device, 2020).

In forensic accounting, supervised machine learning can be used to classify financial data as either fraudulent or non-fraudulent. The first step in using supervised machine learning for forensic accounting is to gather a dataset of financial transactions, which should include both fraudulent and non-fraudulent transactions Once the dataset is collected, it needs to be labeled as either fraudulent or non-fraudulent This labeling process can be done manually by forensic accountants, or it can be automated using existing fraud detection models. Mc Knick (2016:3)

After labeling the dataset, the next step is to train a supervised machine learning model using the labeled data. The model will learn from the labeled data and create a set of rules that can be used to predict whether a new financial transaction is fraudulent or not via to evaluate the accuracy of the model, a separate set of labeled data is used as a testing dataset. The model's performance is evaluated based on how well it can correctly classify new financial transactions as either fraudulent or non-fraudulent. Identification of anomalies in financial statements, forecasting the return of financial statements, identification of possible areas of financial errors, conducting risk assessments one of the most important and important aspects of supervised machine learning in forensic accounting is the choice of algorithm. There are many algorithms available, and each of them has its own strengths and weaknesses. Some commonly used algorithms for classification tasks in forensic accounting include logistic regression, decision trees, random forests, and support vector machines.

Another important consideration when using supervised machine learning in forensic accounting is the choice of features. The accuracy of the model can be improved by identifying the most relevant features or variables that predict fraud. These features can include financial ratios, transaction amounts, dates and locations, among others.

Furthermore, it is crucial to ensure that the data used to train the model is representative of the relevant population this means that the data must be diverse enough to include all possible fraud scenarios that may occur in a realistic environment. It is also necessary to update the dataset to ensure that the model remains relevant and accurate over time Supervised machine learning can be a powerful tool in the hands of forensic accountants to detect and prevent financial fraud. However, it should be used in conjunction with other forensic techniques and should be integrated into the overall criminal investigation process. In addition, it is important to constantly assess the accuracy and effectiveness of the model and make adjustments as necessary (Michal, 2019).

Machine learning offers a dynamic approach to detecting accounting fraud. Through machine learning, forensic accountants can directly access information useful to them from a very large amount of very complex data through multifaceted analysis and thus make decision-making processes more rational (Cahill et al., 2010). On the other hand, thanks to machine learning, accounting fraud detection can be carried out more accurately, so accounting irregularities that were easier to perform become more difficult to perform, and even such irregularities can be completely prevented (Singleton, 2015).

Accounting research conducted to prevent fraud and accounting fraud has recently been based on various statistical methods and machine learning algorithms, mainly instead of classical methods (pools, 2019). Many companies detect irregularities in their structures through machine learning and even protect themselves from losses caused by possible irregularities.

For example, a bank in the United States that receives more than 20 million credit card applications every year is faced with a group of scammers who use stolen and fake identities to apply for hundreds of new card applications for years. The bank's operational teams have long been faced with fraud alerts that require intensive audit and research. However, the solutions for the bank's clients are interactive and come into force after accounting irregularities. New preventive measures taken by the bank against the fraud measures encountered by the bank meant a delay of more than a year for the bank (Data Visor, 2020).

However, there is no year to lose for the bank. The scammers used several different email addresses that were redirected to the same email account by exploiting vulnerabilities in the Gmail system. For example, in the Gmail address". (Point) "Because he could not perceive the sign "abc.def@gmail.com", "ab.cdef@gmail.com", "abcd.ef@gmail.com" all transactions performed by a large number of addresses, such as "abcdef@gmail.com" addressed to the title. Scammers continued to try different ways to avoid getting caught. To prevent the detection of fraud, when applying for a bank credit card in the first week 2. They used different names and emails to apply for the week B card. However, as a result of the bank's use of machine learning, it was decided that IP subnets, devices, operating systems, and browsers that perform transactions remain the same and have not changed. In addition, scammers use the names and addresses of real people living in the United States, which is a special region of China. "126.com use the email domain name". The IP addresses where the applications are processed refer to a single data center in Los Angeles. The bank has taken a comprehensive approach to detect this complex fraud in the application through machine learning.

The solution provided by machine learning has significantly increased the operational efficiency of the bank. Within this framework, the bank has achieved a 25% increase in the detection of fraud incidents through machine learning. It has been found that machine learning is 94% successful in detecting fraud incidents. In addition, operational losses and costs caused by fraud were reduced by more than 15 million dollars (DataVisor, 2020).

In addition, this solution provided by unattended/unsupervised machine learning shown in this example is a solution that can be applied to a large number of cases of the same form of fraud. Machine learning, providing solutions with a high accuracy rate, makes it possible to proactively develop solutions against unknown scams and frauds.

To give another example, there have been many fake users as well as good users of the online world Sunday which operates in more than 40 countries with more than 350 million monthly active users. The Sunday in question revealed suspicious accounts thanks to machine learning. While she was still in the incubation period, by identifying fraudulent registrations, she discovered similar characteristics and behaviors between accounts and revealed deceptive content. Thanks to this, 88% of fake accounts were detected before they could make their first fraudulent transactions. Another example concerns a leading global social trading platform with more than 250 million monthly active users. Scammers have collectively taken over user accounts and collected their contact information without their consent by forcibly sending emails to legitimate users who do not want to receive them, which can also be referred to as "spam". This situation has harmed the company's brands and as a result, significant losses have been achieved for customers. These emails were reduced by 99% through machine learning and 80% of these users were identified at the registration stage (DataVisor, 2020). It is possible to reproduce these examples in question for various and multiple fraudulent transactions.

٣,١ Preparing the environment

We want a selected surroundings setup that will increase ANN-based programs. It requires an effective CPU and/or GPU due to the fact education of an ANN model is a useful resource-eating undertaking.

- devıces

CPU: Intel center – i5 6600k \CPU: AMD Ryzen 5 5600X

GPU: Nvidia GeForce RTX 2060

Ram: pirate revenge LPs 16 GB Dr 4 3200 MHz-

- Software program

Debian 9 "Stretch". GNU/Linux .

- OpenCL (Open Computing Language)
- ML Library/Framework: cuDNN & TensorFlow 1. Zero.0 •
- Language Platform: Python 2 & Python 3
- ML application: DeepQA
- Dataset: Cornell film Dialogs

Why use GPU?

Forensic accounting involves the use of accounting, auditing, and investigative skills to analyze financial transactions and identify potential financial fraud or misconduct. Machine learning algorithms can be applied to forensic accounting to help identify patterns of suspicious behavior or transactions. Kasum (2019:2)

A GPU (graphics processing unit) is commonly used in forensic accounting machine learning because it can accelerate the computation of machine learning algorithms. GPUs are designed to perform multiple calculations in parallel, which is particularly useful for deep learning algorithms that require large amounts of data and complex computations. By using GPUs, forensic accountants can process large amounts of financial data more quickly and efficiently, enabling them to identify potential fraud or misconduct more effectively in addatıon to thıs , GPUs are also useful for visualizing and presenting complex financial data, allowing forensic accountants to gain insights into financial transactions that may not be immediately apparent from raw data. This visualization can help forensic accountants to detect patterns of suspicious behavior and ultimately identify potential financial fraud or misconduct Schooling deep neural networks may be a time-consuming. (Crumbley and Apostolu, 2019:16)

Method. It involves a big quantity of matrix multiplications and Other mathematical operations that if parallelized, can accelerate The calculation time drastically.A single computing device CPU in contemporary scenario may have eight- 10 cores, while a single GPU may have lots of cores Despite the fact that the GPU cores are slower than CPU cores, the big Variety of cores makes that redundant OpenCL (Open Computing Language).GPU: Nvidia GeForce RTX 2060 with Ram LPs 16 GB Dr 4 3200 MHz

Why use TensorFlow?

TensorFlow is a popular open-source machine learning library developed by Google that is used in a wide range of applications, including forensic accounting. Here are some reasons why TensorFlow is used in forensic accounting:

Scalability: TensorFlow is designed to handle large datasets and can scale to handle distributed computing environments. This makes it a powerful tool for forensic accountants who need to analyze large amounts of financial data.

Flexibility: TensorFlow supports a wide range of machine learning algorithms, including deep learning, which is particularly useful for complex financial data analysis tasks.

Ease of use: TensorFlow has a user-friendly interface that makes it easy for forensic accountants to build and train machine learning models.

Performance: TensorFlow is optimized for performance, using parallel computing techniques that leverage GPUs and other hardware to speed up computations.

Visualization: TensorFlow includes powerful visualization tools that allow forensic accountants to explore and analyze financial data in an intuitive and interactive way.

Due to these motives, I have selected the TensorFlow library To construct a ML ANN.

4. IMPLEMENTATION

4.1. Ubuntu 16.04 & nVidia utilities:

I mounted Ubuntu sixteen.04 with a separate /domestic, / (root) and Swap walls on a computing device. Mounted all vital Packages inclusive of Python 2 and Python 3 and different Dependencies that are required. Installed modern-day nVidia pics drivers, as well as installed Cuda and cudNN utilities that offer tensorflow a bridge Among Python and GPU for education a neural community.

4.2.Tensorflow:

Cloned tensorflow from its GitHub repository.Configured tensorflow set up using going for walks ./configure The script in tensorflow listing. Configuration blanketed Specification of the place of cuda set up, cudnn installation, Compute functionality of your GPU, python set up a directory And so on. After configuring tensorflow efficiently, I built a pip python Bundle and established tensorflow as a plugin on my python 3 Set up.

4.3 Implementation

Ubuntu16.04 & nVidia serviceability I installed Ubuntu16.04.7 with a separate/ home,/(root) and exchange partitions on a workstation. Installed all necessary programs similar as Python 2 and Python 3 and other dependences that are needed. Installed rearmost nVidia plates motorists, as well as installed cuda and cudNN serviceability that give tensorflow a ground between Python and GPU for training a neural network.

Tensorflow. Cloned tensorflow from its GitHub depository. Configured tensorflow installation by running./ configure script in tensorflow directory. Configuration included specification of the position of cuda installation, cudnn installation, cipher capability of your GPU, python installation directory etc. After configuring tensorflow rightly, I erected a pip python package and installed tensorflow as a plugin on my python 3 installation.

4.4 DeepQA ChatBot:

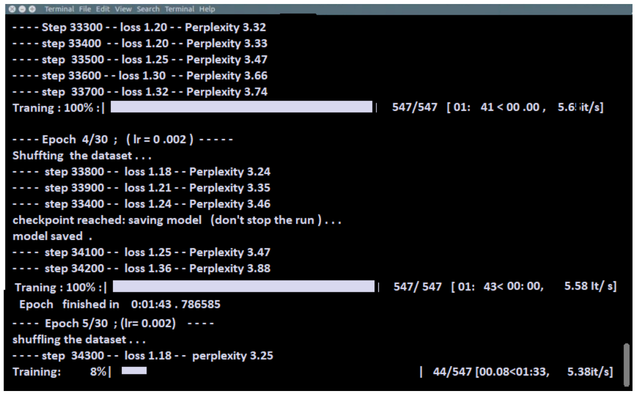
DeepQA is an open-supply Neural Conversational model. It Makes use of an RNN (seq2seq model) for sentence predictions. It's far Based totally on Python and TensorFlow. The benefit of this Software is that it supports a numerous variety of conversational Datasets to be had for research purposes.

DeepQA also presents code to set up a Django internet server That offers the chatbot a nice graphical interface to play with The developer of this application could be very attentive to queries And keeps the mission up to date Due to this program’s versatility and activity, I chose This programme trains an ANN chatbot.

4.5 Lıberary chatbot:

To begin schooling a neural community on the “Cornell movie Dialogs” dataset, I entered the subsequent command:

$python3 main.py --corpus Cornell.



```
- - - - Step 33300 - - loss 1.20 - - Perplexity 3.32
- - - - step 33400  - - loss 1.20 - - Perplexity 3.33
- - - - step  33500 - - loss 1.25 - - Perplexity 3.47
- - - - step 33600 - - loss 1.30  - - Perplexity 3.66
- - - - step  33700 - - loss 1.32 - - Perplexity 3.74
Traning : 100% :| ████████████████████████████ |   547/547  [ 01:  41 < 00 .00 ,   5.6it/s]

- - - - Epoch  4/30  ;   ( lr = 0 .002 )  - - - - -
Shuffting  the dataset . . .
- - - -  step 33800 - -  loss 1.18 - - Perplexity 3.24
- - - -  step 33900 - -  loss 1.21 - - Perplexity 3.35
- - - -  step 33400 - -  loss 1.24 - - Perplexity 3.46
checkpoint reached: saving model   (don't stop the run ) . . .
model saved  .
- - - -  step 34100 - -  loss 1.25 - - Perplexity 3.47
- - - -  step 34200 - -  loss 1.36 - - Perplexity 3.88
 Traning : 100% :| ████████████████████████████ |   547/ 547  [ 01:  43< 00: 00,     5.58 It/ s]
  Epoch   finished in    0:01:43 . 786585
- - - -  Epoch 5/30  ; (lr= 0.002)   - - - -
shuffling the dataset . . .
- - - - step  34300 - -  loss 1.18 - -  perplexity 3.25
Training:       8%| ███                                      |  44/547 [00.08<01:33,    5.38it/s]
```

There are multitudinous distinctive parameters and variables are being Displayed in determine 1. Vindication of them is as follows An time generally means one replication over all the Training data. For case, when you have,000 prints and a Batch length of 100 also the time has to contain,000/ 100 = Two hundred way. The loss measure miscalculations among two tensors, or between a Tensor and 0. Those may be used for measuring the delicacy of a Network in a retrogressionChecking out chatbot:

To test the skilled version and spot how well has it skilled

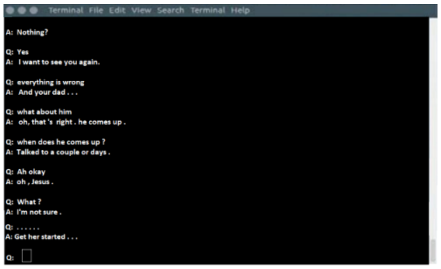
Primarily based on our dataset, I entered the following command:design or for regularization functions. confusion metric in ML is a way to seize the degree of query' a interpretation has in prognosticating(assigning chances To) a many textbooks. It's far associated with Shannon's Entropy. drop the Entropy(query), decreases the confusion. You may end the training at any time by using critical ctrl c within the Outstation. It'll store the interpretation as a. Ckpt report in/ keep the directory And go out of the program. You can renew lessoning from the same step it left off subsequently In case you want to. training an ANN generally takes a atrocious volume of time Depending on the scale of the handed dataset and what number of Ages(one full training cycle) you're running your program For. also the parameters you use as a way to train the ANN goods the training time. It took me about 7 to 8 hours to train an ANN model grounded completely on dereliction parameters wBut through attempting and placing unique values in parameters like

Mastering fee (lr), max sentence length, etc. Started to get me Higher outcomes.I spent extra than 24 hours, in general, to educate extraordinary models To get better effects. Every attempt consisted of 30 epochs with 30 ages and used “ Cornell film converses ” for the dataset. To begin with, it did now not deliver me the correct results.

4.6 Checking out the chatbot:

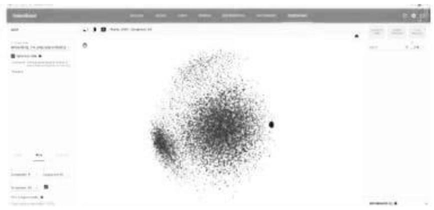
To test the skilled version and spot how well has it skilled Primarily based on our dataset, I entered the following command**: $python3 main.py --test interactive**

It provides a command line interface where you can kind a Question or a message and the chatbot will reply to it.



```
A:  Nothing?

Q:  Yes
A:   I want to see you again.

Q:  everything is wrong
A:   And your dad . . .

Q:  what about him
A:   oh, that 's  right . he comes up .

Q:  when does he comes up ?
A:  Talked to a couple or days .

Q:  Ah okay
A:  oh , Jesus .

Q:  What ?
A:  I'm not sure .

Q:  . . . . . .
A: Get her started . . .

Q:  
```

The replies the bot is giving to questions in determined above. They're no longer exceptional however they're relatively contextual Based totally on the questions requested to it. Education is on a higher dataset and for a longer time with Right learning charge and different parameters can come up with higher Consequences. Now believe we provide this model with a dataset that is composed of Conversations between an assistant worker at the bank and a Consumer. If we train it nicely and lengthy enough then it is going to be Able to effectively make the customer consider that he is speaking to A really legit character and he would trust him sufficiently to expose his Information to him. You can visualize the computational graph, the value of the ANN and word embeddings for our version with TensorBoard, Simply run tensorboard --log dir store/ command. Word embedding is the collective name for a fixed of Language modeling and function getting to know techniques in natural Language processing (NLP) where phrases or terms from the Vocabulary is mapped to vectors of actual numbers in a low-dimensional space relative to the vocabulary length



The embeddings of our trained version can be seen in the Screenshot above. It's miles quite dense. This means it's far a well-skilled A model containing a huge amount of phrase vectors.

5. Forensic acquisition and evaluation

After training a functional neural community that could deliver out First rate output, its time to forensically analyze the machine to find Artifacts that help us decide that the gadget was utilized in Generation and testing of a neural network based on TensorFlow.

A. Gear used:

- **LiME**: “Linux memory extractor” (LiME) is used toTake stay RAM dumps in. Lime and . Raw codecs.

- **Rufus**: To create a bootable Ubuntu 16.04 USB Thumbdrive.

- **Disks software**: it's far part of the Ubuntu live device that Helps you to create images of various partitions or whole

Disk.

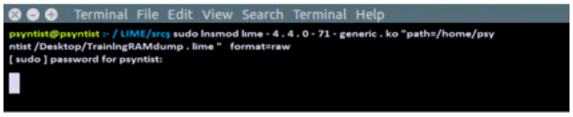
• **EnCase**: EnCase is used to research disk pix and RAM dumps to discover applicable artifacts and to make a Record primarily based on findings and different technical Facts about the machine.

Live reminiscence seizes with LiME:

LiME is a Loadable Kernel Module (LKM) that allows For volatile memory acquisition from Linux and Linux-based totally

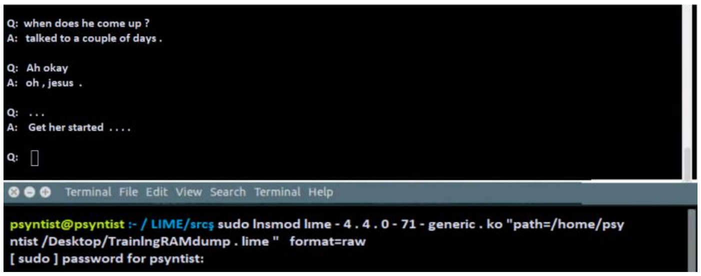
Gadgets.

LiME utilizes the insmod command to load the module, Passing required arguments for its execution. After cloning the supply code of LiME from GitHub, it was far Had to make a kernel module well-matched together with your Linux **Kernel.** You can't load a kernel module this is made for Every other kernel in your kernel. It can be fatal in a few cases for The OS. I loaded the LiME kernel module within the kernel whilst the DeepQA program became in schooling mode



```
psyntist@psyntist :- / LIME/srcş sudo Insmod lime - 4 . 4 . 0 - 71 - generic . ko "path=/home/psy
ntist /Desktop/TrainingRAMdump . lime "   format=raw
[ sudo ] password for psyntist:
```

After taking the RAM dump whilst the software changed into in schooling Mode, I placed the software in trying-out mode and once more took a RAM Sell off in an equal manner.



```
Q:  when does he come up ?
A:   talked to a couple of days .

Q:   Ah okay
A:   oh , jesus  .

Q:   . . .
A:   Get her started  . . . .

Q:  
```

```
psyntist@psyntist :- / LIME/srcş sudo Insmod lıme - 4 . 4 . 0 - 71 - generic . ko "path=/home/psy
ntist /Desktop/TrainIngRAMdump . lime "   format=raw
[ sudo ] password for psyntist:
```

So now we've got specific RAM dumps. One while the The system turned into schooling mode and one at the same time as the device changed into in Checking out mode

- TrainingRAMdump
- TestingRAMdump

5.1 Disk acquisition with 'Disks' utility:

"Disks" is a device that comes preinstalled with Ubuntu 16.04. It lets you manage your hard disk partitions. You could create

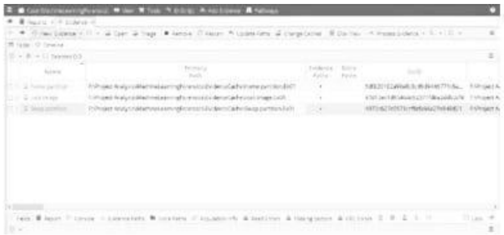
New walls, edit partitions, decrease, extend, mount, unmount And take logical images of walls.Img format. I created an Ubuntu sixteen.04 live bootable USB thumb force And booted it up on my machine. I released the Disks application and decided on /the home partition. Clicked on the settings icon on left and decided on 'create logically Photograph' the partition and provided the place to keep a bit by-bit photo of /home partition

I

I did the equal process with the final walls Respectively, / (root) and swap. So now we've logical pics of all 3 walls used On Ubuntu with the purpose to be loaded on EnCase for investigation. The cause to accumulate those walls is defined underneath: /**domestic**: DeepQA program is hosted on this partition as well As RAM dumps I took with LiME are saved here. / (**root**): installation of TensorFlow and other dependency Packages had been finished in this partition. Plus this listing is the Parent of all directories on Ubuntu. **swap**: swap is used for paging. So it'd have some Volatile data stored that is probably useful for the investigation.

5.2 Forensic evaluation on EnCase:

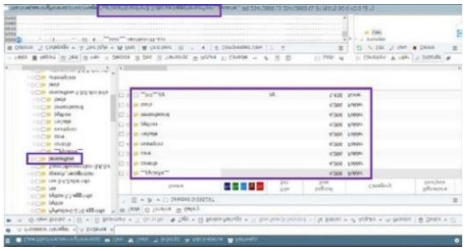
Now comes the maximum thrilling part of this undertaking. Reading the RAM dumps and tough disk snapshots to discover Relevant artifacts. I selected EnCase to analyze the evidence because EnCase Offers nation-of-the-art answers for proof analyzing, Processing and document generating. The interface is also smooth to Use and easy. The biggest gain to apply EnCase is that it can be noted in The court docket of law in u.S., India, and other primary countries. I created a new case on EnCase and entered appropriate Statistics which include the name of the case, case-wide variety, the examiner Name case id and so on. After creating the case, I delivered evidence documents one by one. Firstly, I began by including the logical photo of /home Partition. After including the picture of /the home partition as an Evidence document, it's time to acquire equal evidence. EnCase Makes .E01 photo of the uncooked photo the proof we Furnished in acquiring phase. After acquiring the proof picture, I put the acquired Evidence picture on processing. Decided on suitable processing Options like system data Parser, file Carver, private Facts extractor, Linux Artefact Parser, etc. I followed the same procedure for acquiring and processing For subsequent logical pix, / (root) and switch. Processing swap partition did now not give any labeled Facts changed into shown as unallocated space however, a few uncooked facts Can be determined from that unallocated area. After including, obtaining, and processing all proof files **EnCase** evidence window seems like this:



6. Findings:

I began the evaluation of evidence and discovered some concrete Artefacts explained under:

1- Tensorflow set up place: One of the maximum number one and most important artefacts is to discover Out of TensorFlow is set up at the machine. TensorFlow is a Python library. So, first, take a look at the region Of Python installation and then look for TensorFlow interior it. On any Linux-based total OS packages are installed under /usr Listing so it is the first listing one needs to bear in mind to Examine the Python setup. Tensorflow is hooked up under /usr/local/lib/python3.Five/distpackages/tensorflow directory



Interestingly, this directory also incorporates a few thrilling Python libraries that may be used as a part of ML software. Together with speech_recognition, pyttsx, and many others.

2-sequence keyword:

Seq2seq (sequence to sequence) is a class of tensorflow that Is utilized in growing a sequence to sequence, RNN (recurrent

Neural network) version.

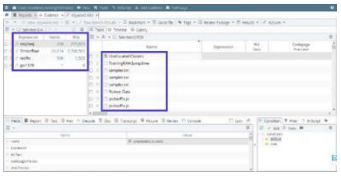
3- DeepQA application is based totally on seq2seq modelling and is a Recurrent neural network. So the possibility to locate this class

The used in introduction of the model is excessive. Netflix key-word: Phrase Netflix become a part of our dataset I used to train our ANN. So the use of this as a keyword to look to peer if we are able to locate It in RAM dumps or on swap partition RTX 2060:

If education of ANN application become achieved with tensorflow and GPU, it's going to encompass the name of the GPU used within the training As a minimum somewhere in volatile data or in parameters of Tensorflow.

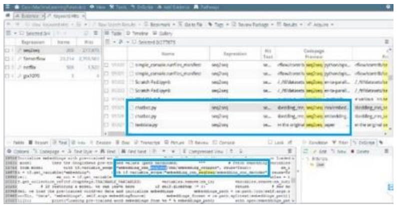
4- Key-word hits:

It takes a good amount of time to investigate all evidence files For the provided keywords to EnCase. However it tests all Evidence files thoroughly and even shows if key-word hits become Discovered in an unallocated area. After the processing of searching for key phrases finishes, EnCase shows you all of the keyword hits in a single window of Key phrases. It shows the number of documents and variety of hits the Key-word has were given right next to the name of key phrases. It can be Seen within the screenshot underneath.



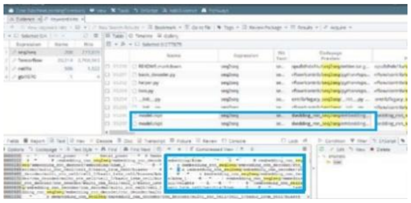
Seq2seq key-word hit:

Exceedingly seq2seq keyword got 277,875 variety of hits In all evidence pics. That means it has been used a lot in the 208 Range of files. I analyzed a number of the documents and located the following outcomes. Discovered the python script record of DeepQA chatbot.Py Containing the seq2seq keyword. It could be seen that tensorflow Class seq2seq magnificence is used within the code of this document.

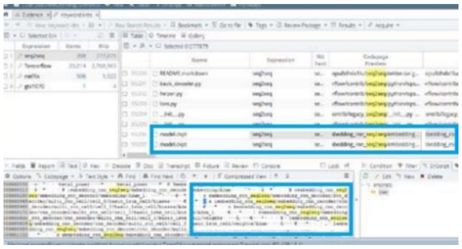


The equal key-word changed into also found inside the compiled chatbot Report chatbot.P.C it confirms that the script became certainly ran at

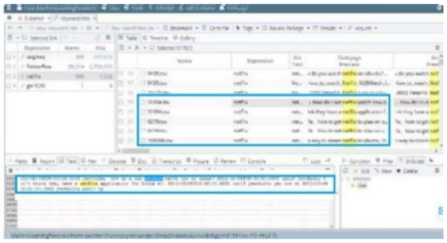
Least once on the machine. The p.C (Python compiled) document best Generates as soon as the program executes at the least as soon as



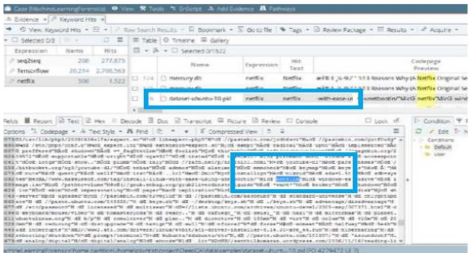
The key-word seq2seq changed into also determined within the version.Ckpt record Of our chatbot. This additionally confirms that the training of an ANN Become dedicated. Because we realize that version document most effective generatesAfter you begin training a neural community.



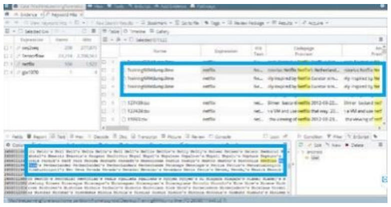
Netflix keyword hit: I found a Netflix keyword hit in some dataset documents (.Tsv). We Can see that the word has been cited in a verbal exchange Between parties inside the document content material.



Discovered Netflix key-phrase in a dataset.Pkl record. The pickle Module (.Pkl) implements a vital, but effective Set of rules for serializing and de-serializing a Python object Shape. Tensorflow uses .Pkl files at the same time as this gadget is in Finding out mode to offer quick serialized outputs.

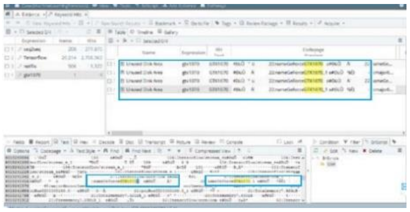


One exciting discovery for this keyword become in the Training RAM dump record that was captured at the same time as the application was Education. This artifact confirms that the dataset that contained This key-phrase has become significantly applied in training this gadget



Based totally on the artefacts i discovered regarding Netflix key-phrase, I Can verify that string ‘netflix’ changed into a part of dataset and the

Dataset come to be used at the same time as this system have become training. RTX 2060key-phrase hit The RTX 2060changed into determined on switch partition. For the reason that the swap partition is taken into consideration as unused disk place, EnCase indicates it as one unmarried uncooked file. Switch file is used for paging. So due to the fact, the keyword is Referred to here together with strings like tensorflow inside the Content, we will finish that GPU acceleration became used to Teach neural networks the usage of tensorflow.



7. Consolation

An ANN with the help of tool reading has been given Higher with the advent of Google's open delivery system Studying the library TensorFlow. After finding the applicable artifacts in the investigation of The proof photographs, I will finish a tool-learning Application based totally on Tensorflow come to be educated as well as performed On the gadget. These findings can be used as a reference in future instances to Find out or perceive the usage of gadget-mastering libraries, Algorithms, strategies, and so forth. However, a lot of studies and paintings desire to be completed in This subject. A proper and deeper evaluation of volatile statistics Might be useful as well as greater in-intensity evaluation of neural Networks would possibly assist us to get more acquainted with the system Reading applications within the scope of digital forensics.

8. Results vıa recommendations

Scams and frauds have increased significantly in recent years, especially in light of the presence of all these developments, technology and the digitization world, it has become easy to commit economic crimes without leaving the site, even in light of all these facilities, it was natural to increase financial crimes, money laundering and others . And because the detection of accounting frauds is very difficult due to the complexity of the processes required by the process of proving the crime, especially in the presence of technologies such as social engineering and open source (Linux and Unix), it became easy to commit a crime while it is difficult to determine who did it, so the concept of judicial accounting appeared and its importance increased to detect the types of crimes committed, thereby , It was a good idea to use advanced techniques to facilitate and identify the culprit using machine learning techniques and by developing codes and by introducing specific programs that enable to identify the perpetrators of economic crimes effectively .

Machine learning is a powerful tool that has the potential to revolutionize the field of forensic accounting by allowing criminals and financial fraud to be detected more efficiently and accurately than traditional methods. By leveraging massive amounts of data and advanced algorithms, machine learning models can analyze patterns and anomalies in financial transactions that may indicate criminal activity.

One area where machine learning has been particularly effective is the detection of money laundering, a common tactic used by criminals to hide the proceeds of illegal activities. Machine learning models can be trained to recognize patterns of suspicious financial behavior, such as unusually large or frequent transactions, transactions involving high-risk countries or individuals, or transactions that deviate significantly from the normal behavior of a particular account.

In addition to detecting money laundering, machine learning can also be used to identify other types of financial crimes, such as fraud, embezzlement and insider trading. By analyzing data from multiple sources, such as financial data, trading records, and social media, machine learning models can uncover hidden relationships and patterns that may be indicative of criminal activity.

Machine learning models are able to analyze huge amounts of data with high accuracy and speed, which allows them to identify patterns and anomalies that a forensic accountant may miss and machine learning algorithms can process large amounts of data quickly and automatically, reducing the amount of time and resources needed to investigate financial crimes. This can help law enforcement agencies prioritize cases and allocate resources more effectively and machine learning models can also be trained to identify subtle patterns and anomalies in financial statements that may be indicative of criminal activity.This helps to detect fraud and other financial crimes more quickly and accurately than traditional methods.

Machine learning can be integrated with other technologies such as blockchain and big data analytics to provide a more comprehensive view of financial transactions and identify suspicious activity more effectively.despite the progress made in using machine learning in forensic accounting, there are also some challenges and limitations that you should be aware of. For example, machine learning models are only as good as the data they are trained on, and biased or incomplete data can lead to inaccurate results. In addition, machine learning algorithms may be vulnerable to manipulation or hacking, which may compromise the integrity of the results.

Refarnces

Baruch Lev, Yaniv Konchitchki, and Clive Lennox, "The forensic accountant," Journal of Accounting Research, vol. 54, no. 2, pp. 397-416, 2016.

Marian Zgajnar and Maja Zumer, "Data analytics and forensic accounting: A bibliometric analysis of research trends," Journal of Forensic Accounting Research, vol. 3, no. 1, pp. 148-168, 2018.

Alain R. Biem, "Data mining and forensic accounting," Journal of Forensic Accounting, vol. 4, no. 1, pp. 67-80, 2003.

Cemal Kaya and Mehmet E. Yaşar, "Application of data mining in forensic accounting: A research note," Journal of Financial Crime, vol. 23, no. 4, pp. 1004-1015, 2016.

Wen-Chih Lee, Ying-Ming Wang, and Han-Shen Chen, "Fraudulent financial reporting detection using data mining techniques," Journal of Forensic Accounting Research, vol. 1, no. 1, pp. 1-26, 2016.

Kathryn Rudie Harrigan and W. Robert Knechel, "Using data mining to detect fraud: A review of research and implications for the future," in The Routledge Companion to Accounting and Risk, Routledge, 2016, pp. 299-317.

Mohd Rizal Palil and Rizal Ahmad, "The effectiveness of data mining techniques in detecting financial statement fraud: A review," Journal of Financial Crime, vol. 26, no. 4, pp. 1184-1201, 2019.

Chia-Jung Chien, Chi-Hung Lin, and Kuei-Yang Chang, "Fraud detection using data mining techniques," Journal of Money Laundering Control, vol. 20, no. 1, pp. 22-39, 2017.

W. Robert Knechel and Anthony J. Catanach Jr., "Using data analytics to detect fraud," Strategic Finance, vol. 98, no. 8, pp. 44-49, 2017.

Dan Zhang, Zengquan Li, and Qiang Shen, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," Intelligent Systems in Accounting, Finance and Management, vol. 25, no. 1, pp. 1-19, 2018.

Richard Overill, Machine Learning Forensics for Law Enforcement, Security and Intelligence. Springer, 2021.

Sinan Kockara, Ali Dehghantanha, Kim-Kwang Raymond Choo, and Richard Jiang, "Machine learning in digital forensics: A review," Expert Systems with Applications, vol. 131, pp. 415-441, 2019.

Elie Bursztein, Vikas Mishra, and Anna-Kaisa Pietiläinen, "Machine learning for network intrusion detection: Approaches, datasets, and open problems," ACM Computing Surveys, vol. 53, no. 2, pp. 1-39, 2020.

A. S. Sallam, K. Salah, A. Shalaby, and A. Hassanien, "Intelligent digital forensics: A review," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 7, pp. 5987-6011, 2021.

Steven Wierckx, Tim Stakenborg, and Wim Lamotte, "Towards machine learning-assisted digital forensics: A review," Journal of Network and Computer Applications, vol. 135, pp. 28-48, 2019.

Hamza Aldabbas, "Machine learning in digital forensics: A systematic review," Journal of Digital Forensics, Security and Law, vol. 14, no. 2, pp. 23-46, 2019.

Danfeng Yao, Weiqing Sun, and Yuan Hong, "A survey on deep learning for cybersecurity," IEEE Transactions on Big Data, vol. 7, no. 1, pp. 3-35, 2021.

Saman Zonouz, Kevin Hamlen, and Bhavani Thuraisingham, "Machine learning in cybersecurity: A comprehensive review," IEEE Communications Surveys and Tutorials, vol. 20, no. 4, pp. 2691-2730, 2018.

Nidhi Arora, "Machine learning in cybersecurity: Applications and challenges," Journal of Cybersecurity, vol. 5, no. 1, pp. 1-17, 2019.

M. Farhan Malik, Syed Ali Hassan, Adeel Baig, and Asif Irshad Khan, "Machine learning in digital forensics: A survey," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 11, pp. 10679-10695, 2021.

R. C. E. Tan and C. Y. Suen, "Machine learning in digital forensics: A survey," in Advances in Digital Forensics XIV, Springer, 2018, pp. 3-16.

Alaaeldin Amin, Mohammad S. Obaidat, and Mohammad A. Al-Fayoumi, "Machine learning techniques in cybersecurity: A review," Journal of Network and Computer Applications, vol. 107, pp. 71-99, 2018.

Hui Yang, Xunhua Wang, Guohui Li, and Fang Liu, "Deep learning for digital forensics: A comprehensive review," Digital Investigation, vol. 29, pp. 94-112, 2019.

Brian D. Carrier, "Machine learning for digital forensics," in Digital Forensics and Cyber Crime, Springer, 2013, pp. 3-14.

Dimitris Gritzalis, Dimitris K. Kalofonos, and Angelos D. Keromytis, "Intelligent techniques for digital forensics," in Handbook of Research on Computational Forensics, Digital Crime, and Investigation, IGI Global, 2009, pp. 110-131.

Sadiq Hussain, Vassil Roussev, and Golden G. Richard III, "Machine learning for digital forensics: A critical review," ACM Computing Surveys, vol. 51, no. 5, pp. 1-32, 2018.

Anjali Taneja, Utkarsh Gupta, and M. D. Tiwari, "A review on machine learning techniques for digital forensics," in Proceedings of the 4th International Conference on Computational Intelligence in Data Mining, Springer, 2021, pp. 173-183.

Kyriakos E. Psarakis and Constantine E. Spyrou, "Machine learning techniques in digital forensics," Journal of Forensic Sciences & Criminal Investigation, vol. 6, no. 2, pp. 1-7, 2019.

Brian D. Carrier and Erin E. Becker, "Machine learning and digital forensics," Digital Investigation, vol. 16, no. 2, pp. 70-80, 2016.

Ibrahim A. Albluwi and Matthew S. Wilson, "Machine learning in digital forensics: An exploratory study," in Proceedings of the 2017 10th International Conference on Developments in eSystems Engineering, IEEE, 2017, pp. 279-284.

Soumya Paul and Gaurav Gupta, "Machine learning in digital forensics: A systematic mapping study," Digital Investigation, vol. 33, pp. 1-17, 2020.

Zhizhong Zhang, Wenqian Dong, and Wei Jiang, "Machine learning in digital forensics: A survey and future directions," Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 7, pp. 2749-2774, 2020.

Kyriakos E. Psarakis and Constantine E. Spyrou, "Machine learning in digital forensics: A critical review," IEEE Access, vol. 7, pp. 51038-51060, 2019.

Jinhua Guo, Jiao Sun, Zhiwei Wang, and Xinhao Wu, "A comprehensive review on machine learning in digital forensics," Journal of Intelligent & Fuzzy Systems, vol. 39, no. 2, pp. 1721-1736, 2020.

Dong Sun, Cong Wang, and Lei Zhang, "A survey on machine learning for intrusion detection," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 4, pp. 476-491, 2018.

Arash Habibi Lashkari, Mohammad Hashemi, Amirreza Niakanlahiji, and Ali A. Ghorbani, "A survey on intrusion detection using machine learning techniques," Journal of Network and Computer Applications, vol. 98, pp. 18-38, 2017.

M. H. Bhuyan, M. K. Islam, D. K. Bhattacharyya, and J. S. J. Toral, "A survey on feature selection techniques in intrusion detection systems," Computers & Security, vol. 51, pp. 1-14, 2015.

Andrea Continella, Giovanni Lagorio, Antonio Lioy, and Andrea Saracino, "A systematic survey on the detection of malware using machine learning techniques," Journal of Computer Virology and Hacking Techniques, vol. 16, no. 1, pp. 1-38, 2020.

Flavio Toffalini, Michael N. DeMott, and Lorenzo Cavallaro, "Machine learning for malware detection: A survey," ACM Computing Surveys, vol. 53, no. 1, pp. 1-36, 2020.

Md. Rakibul Islam and Md. Arafat Hossain Khan, "A survey on the application of machine learning techniques for intrusion detection," Journal of Information Security and Applications, vol. 47, pp. 102573, 2019.