International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 9 Issue 4, April 2022

ISSN: 2394-4404

Application Of Deep Learning In Fraud Detection In Payment Systems

Yakob Ali Mohammed

Post Graduate Student of Ferris State University

Abstract: ***E-payment systems are currently highly susceptible to fraud, hence the demand for enhanced security detail of the various payment systems in use today. Businesses need to bolster their security systems to prevent unauthorized access to organization data, which constitutes several adverse impacts such as theft, and data loss once accessed. Deep learning can be used as a leverage in this approach, and which is responsible for enhancing security of credit card payments. Deep learning helps in detecting real time attempts of unauthorized penetration in an organization's information system. Machine learning is an essential approach in culminating cyber security issues in the world today. This paper addresses the various types of credit card frauds which include pin shimming, skimming and card cloning especially during this era of high technology. This paper also addresses the various deep learning techniques such as IPS and IDS which are currently the most efficient and effective fraud detection techniques. However, these techniques are attributed to long implementation processes and hefty financial burdens, hence, have not been successfully established in a significant number of organizations. It is, therefore, essential for organizations to bolster their security details by shifting from the conventional data protection approaches to the deep learning techniques such as IPS and IDS to ensure real time risk detection and execution of the necessary security measure to mitigate the malice.***

Keywords: Technology: Data protection, Security: Deep Learning, Upgrade: Cyber-security, Transaction: Intrusion Detection, System

I. INTRODUCTION

Advancements in technology in the current world have resulted in various improvements across various sectors, such as security, sharing of information, and upgrades on how business operations are executed, including making payments involving large amounts of money. Although technology has resulted in various positive impacts on business, these advancements are also attributed to many cases involving hacking and fraud where companies and individuals lose significant amounts of money through technology. The increased instances of fraud have necessitated organizations to generate various approaches that can be used to mitigate fraud arising from technological advancement, and this includes deep learning approaches involving fraud detection, especially in payment systems. According to Ali et al. (2019), using deep learning to detect fraud in various automated payment systems shall significantly reduce these cases. Besides, deep learning in fraud detection in payment systems addresses the different techniques used by fraudsters through the internet and browsers, how these fraudsters maliciously gain access to sensitive personal and organizational data, and how they end up transferring funds maliciously or interfering with the payment systems. As a result, it is necessary to protect existing payment systems using highly sophisticated approaches involving current technologies to keep these systems safe and secure from malicious access by fraudsters.

Transaction systems that require advanced data protection should ensure enhanced fraud detection systems to keep their data safe and free from malicious access by unauthorized users. Currently, there have been increased cases of cyber security involving malicious access and use of individual and organizational information. Organizations need to reinforce their security systems to protect their data, primarily through deep learning detective systems that can detect malicious attempts in advance before access, from where the necessary security measures can be taken with immediate effect.

ISSN: 2394-4404

II. CYBER SECURITY

Due to the current technological advancements, cyber security has become one of the most demanding issues that need to be addressed in the currently technology-dominated world. The manner in which people shop online, make payments, and send money internationally has motivated the interest of various types of hackers who wish to invade the payment systems objectively to acquire funds for different clients in their online payment processes. As a result, companies need to bolster the security of their systems to prevent their information and that of clients from external access that might lead to fraudulent activities or malicious use of a company or individual information. Compromising the security of credit cards belonging to clients is a severe concern that needs to be addressed through various software engineering approaches from which security can be bolstered and prevent attacks from fraudsters (Fiore, 2019). This process involves shifting the conventional security parameters organizations use and adopting the more secure and highly intrusion-detective systems that include the IPS and the IDPs.

III. TYPES OF CARD PAYMENT FRAUDS

There are several card payment frauds across the world today. To protect against fraud in payment systems, various approaches can be used to protect card data since a significant percentage of all payments involve user details encrypted in the cards. Some of the most common types of fraud involving cards include Pin Shimming, Card Cloning, and Card Skimming (Ali et al., 2019). According to Ali et al. (2019), shimming has become one of the riskiest threats to payment systems involving the usage of cards today. Ali et al. (2019) infer that shimming can be called an update of the skimming technique, which consists of a process where malicious individuals, especially thieves, attach devices known to them on the credit card readers. This act most occurs in places involving cards for payments, such as gas stations. The malicious users, who in this case refers to thieves, acquire the user's credit card details through the process whereby the attached devices transfer the payment and bank information belonging to the user from the credit card during the magnetic swipe process. Initially, several gas stations had established a technique involving the use of chip-enabled credit cards, although this approach was attributed to several vulnerabilities regarding data leakage. However, this technique is no longer effective following the current technological advancements. This is due to the increased efforts by fraudsters to forcefully acquire access to the information stored in the cards, which involves details of the user and their bank account details (Ferraq, 2020). As a result, hackers came up with the shimming approach.

Mobile-related fraud has also become a constant issue of concern, an approach currently associated with the use of malware. This approach is among the commonly used techniques to acquire the payment details of an individual. Some of the other constantly used methods of payment fraud include the use of fake applications whose primary purpose is to obtain the user's details from where their accounts can be accessed. Hackers are currently engaging in increased use of acquiring account details through mobile phones because mobile phones have grown to become the commonly used payment devices amongst different individuals through mobile banking. This factor has been facilitated by the increased usage of online businesses, from where customers can order and pay for their goods through their banks by mobile phones. Besides, mobile phones are the most commonly used devices to make payments, primarily due to their affordability. As a result, hackers and fraudsters have focused more on hacking user details through mobile phones. Hacking through mobile phones is a significant advantage to the hackers since this approach negates various tracking procedures that target persistent identification. Unlike these conventional approaches, hacking consumer details through mobile phones helps the hackers evade the identifications and alarms made once the same device is used to acquire penetration into a different account since, in most cases, each mobile device is connected to a single account from where the user makes all the payments.

Mobile related attacks, as used mainly by various fraudsters, involves multiple approaches that, in most cases, consist of account takeover where a malicious user acquires various details belonging to a particular mobile user's bank account from where they can change the security credentials required and retail the money for their use while blocking the other user. Other instances include fake applications. In other cases, approaches such as phishing and fraudulent websites are used to trap customers into paying through incorrect details, which are provided by scammers (Ali et al., 2019). As a result, various methods have been established to counter these hacking approaches relating to mobile phone usage. One of the most effective approaches used is the adoption of machine learning (ML), which was developed and implemented to counter fraud and control access (Ali et al., 2019). The use of machine learning in enhancing security involves the establishment of authentication mechanisms that are used to verify the identity of the users. Besides, machine language prevents malicious access to mobile phone accounts through access control measures due to the high rates and probability of changing ownership due to the mobility of mobile phones.

IV. SOFTWARE ENGINEERING CHALLENGES OF DEEP LEARNING IN IMPROVING PROTECTION OF PAYMENT SYSTEMS FROM FRAUDSTERS

Although Machine Learning has proven to be a fruitful approach to protecting payment systems from malicious access by fraudsters, the process is affected by various challenges. According to Ali et al. (2019), Machine Learning proved to be a current practical approach toward enhancing the security levels of payment systems. For instance, some of the areas where Machine Learning has realized effectiveness include various learning institutions and some of the outstanding technology companies in the world (Arpteg et al., 2018). This effectiveness has resulted from increased technological research. Besides, the competition for innovativeness across different companies has also significantly facilitated the enhancement of the security levels

of various payment systems. However, the Deep Learning elements have been attributed to multiple critical concerns, including the techniques for developing Deep Learning systems (Arpteg et al., 2018). Due to this reason, among others, various challenges associated with the Deep Learning approach to enhancing payment security have been discussed below.

Big companies engaging in software production are establishing more advanced and sophisticated software through various restructuring processes that involve the use of advanced artificial intelligence techniques. Some of these companies include Facebook, Google, and Microsoft. However, in relatively more minor companies, various challenges such as appropriate infrastructure and financial resources have always been challenging in developing and establishing advanced protection systems to counter the risks of fraud by malicious parties (Fiore, 2019). According to Arpteg et al. (2018), other areas challenging the development and establishment of advanced payment protection procedures include the need to have a large team of professionals with sufficient development skills and production. To counter these challenges, such companies require the incorporation of reviewing policies to evaluate the validity and effectiveness of their development and establishment processes of various security software, which involves advanced debugging techniques. As a result, another challenge affecting the development of security software for the payment systems is the lack of sufficient debugging processes to enhance the security of the payment systems through protection from malware and other threatening software that might attack the systems, thus, compromising their security information regarding client payment details.

Effort estimation has also been identified as a worthwhile setback in developing and establishing more secure deep learning systems. This challenge involves the inability to approximate the required development, testing, and debugging time for the DL systems in most organizations (Arpteg et al., 2018). Besides, financial challenges have also served as a significant challenge in establishing better DL systems, especially the project BOT. The inaccuracy experiencing the expected time and resources for developing these software has necessitated companies to call out their already initiated development processes for DL systems, thus embarking on continued use of less secure and efficient payment security systems that compromise user information fraudsters (Arpteg et al., 2018). Therefore, these development processes' indefinite time and resources have led to significant challenges in establishing advanced DL systems since milestones and the project course cannot be set and facilitated to the latter.

Another software engineering challenge affecting the development and establishment of DL systems includes the insufficient transparency associated with the process. This means that organizations fear that some of the techniques and security patches embedded in the DL systems might be monitored by the development team, who might decide to use this knowledge against the company and acquire access to the DL systems, thus, accessing client information without authorization. Some of the factors contributing to the leakage in data during the development of the DL systems include the imperfect and noisy nature of the established security systems. This lack of transparency in these systems has been thought to have been brought about by black-box models (Fiore, 2019). This aspect has also been triggered by the lack of sufficient direct modest explanation of the underlying functionalities of various security DL processes.

V. INTRUSION DETECTION AND PREVENTION SYSTEMS (IPS AND IDPS)

It has been noted that data protection and how the data flow is controlled in DL systems has been a crucial issue of concern during the process of sharing data across different networks or systems. This challenge has necessitated the development of more secure data sharing and transfer systems to ensure the security of client data to avoid issues of acquiring access by parties with malicious intent. To counter the problem of intrusion, intrusion detection is executed in a system to evaluate its level of security. This process involves keeping a close check on all the events running and taking place in a computer system and identifying cases of violation and imminent threats to the system, from where the appropriate security actions against this interference can be implemented. The IDS software is specially designed to automate the detection process where malicious or unwanted incidences can be detected (Patel, Qassim & Wills, 2010). The Intrusion Prevention System is also specially designed to stop various incidences that are deemed unwanted in the system. In some cases, the functionality of IPS is switched to match that of the IDS.

It is essential to embed current DL systems with advanced IPS and IDPs that can detect, identify, and stop unwanted processes. These systems can detect malicious or unauthorized access to a system and prevent them appropriately to safeguard the information transmitted in the system (Patel, Qassim & Wills, 2010). Besides, this security approach effectively detects violations of the various rules, regulations, and policies established to govern the transmission of data within the system. Thus, unwanted requests and processes can be aborted immediately. This approach is effective and efficient in techniques involving the communication and sharing of data and files in bulk across companies and organizations. Additionally, IDPs are embedded with advanced technology that can help identify the nature of malicious attempts into the system by evaluating the characteristics and frequency of the incidences (Scarfone & Mell, 2010). Another technique IDPs use to enhance security of data in these systems includes changing security measures and details once a malicious attempt is detected. Besides, these IDPs have the capability of following up on the incidence to identify its various features.

Although the IPS and IDPs have similar functionality, one is preferred in various incidences to the other. The IPS are more applicable in aborting the execution of an unwanted incidence in the system immediately after detection. The most basic technique of how IPS executes its functions is that it aborts the attack through measures such as terminating the network connection (Patel, Qassim & Wills, 2010). Some of the attackers' attributes that are monitored and consequently stopped include IP address and the offending user account.

Secondly, the IPS can provide security to the system by altering the security environment. This process might involve the IPS, to a considerable extent, changing the configuration settings of a network firewall to counter access the incidence of other related incidences. Thirdly, the IPS performs its security functions by altering the attack's content. Through process involves interfering with the composition of the attacker and changing various features to render the attacker benign (Scarfone & Mell, 2010). For instance, IPS are involved in ejecting infected file attachments, especially from means that include emails, where most communication is done through attached files. In this way, the IPS interferes with and significantly destroys malicious software or content trying to access the data in the files.

The IDPs detection methodologies are executed through various approaches that include signature-based and anomaly-based procedures. Another commonly used malware detection technique in IDPS is stateful protocol analysis. These technologies are sometimes used independently or integrated to operate as a single system. Once these methodologies are integrated together to execute their functions collaboratively, advanced, better, and more effective detection against malicious access or access by any unauthorized party is achieved. Signature-based approaches involve detecting malicious access by analyzing and comparing the available signatures to see any strange signatures, which imply that the system is being attacked externally.

Anomaly-based detection procedures involve cases where the profiles are either static or dynamic. Static files refer to the ones that remain unaltered, and changes to them only occur once the IDPS is commanded to execute such a function. On the other hand, a dynamic profile refers to the one that is repeatedly updated due to the different events directed to it. However, static profiles are attributed to recurrent issues of inaccuracy, thus the need to ensure that they are regenerated periodically (Scarfone & Mell, 2010). This characteristic grants the other type of dynamic shape an added advantage in such scenarios. However, these profiles are attributed to crucial risks of malicious access due to their susceptibility to evasion attempts. Dynamic profiles are challenged by the fact that the attacker can keep their penetration of the system by executing occasional malice.

VI. AN ILLUSTRATION OF AN INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)

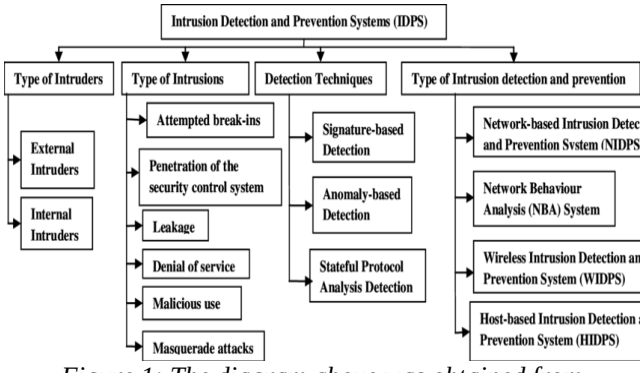

Figure 1: The diagram above was obtained from https://www.researchgate.net/figure/Sub-systems-of-Host-based-Intrusion-Detection-and-Prevention-System_fig2_271070098

The above diagram illustrates the intrusion detective and prevention systems and how the process trickles through the system to detect and identify any new or malicious access of the information. The diagram illustrates how the three techniques of IDPs can be integrated in a single system to work collaboratively in eliminating any slight risk of invasion from attackers. The system detects malice from afar and either aborts that process, or cuts down the network to prevent any more access to information (Jayanta, 2013). The system also analyzes each request and its characteristics. In this way, the system can detect and follow up attackers.

Consequently, the malicious invader might continue the frequency of invasion of the system, a process that can lead to him acquiring a substantial amount of information from the system. However, the anomaly-based IDPs are also challenged by the issue of false positives due to the underlying problem arising from benign activities (Scarfone & Mell, 2010). This issue mainly occurs in diverse and dynamic environments.

Stateful Protocol Analysis is a security improvement approach that incorporates a comparison of predetermined profiles that are specially designed to monitor and identify instances of deviations in a system. This approach uses vendor-developed techniques whereby the IDPs establishes a thorough examination of the state of the network. The stateful protocol analysis involves pairing requests with responses in the system whereby before executing the sent requests, the FTP (File Transfer Protocol) can evaluate their nature before allowing various commands to be completed. Stateful protocol analysis effectively enhances security in that it can address random sequences of commands in a system (Patel, Qassim & Wills, 2010). For instance, this approach can identify repeatedly issued commands and identify the authenticator in different operations.

Although ID/PS has been proven to be some of the most secure approaches to protecting data, these processes have been increasingly demanded, although their security detection and enhancement capabilities can be bolstered using various supporting tools and intelligent methods. As a result, their use requires integration with Machine Learning, Artificial Intelligence, data mining, DL, and autonomic computing (Patel, Qassim & Wills, 2010).

VII. CONCLUSION

In conclusion, information security is an essential aspect of any business so as to keep their data sharing and transfer systems safe and secure from access from unauthorized or malicious people. Organizations contain sensitive data that needs to be kept safe and free from external access to avoid malicious use such as manipulation, deletion, and use for malicious activities such as identifying the secrets of an organization leakage of other various sensitive data. Organizations need to implement highly secure systems, especially in the payment procedures, to ensure that none of the client's or organizational data is accessed maliciously. Unauthorized access to client payment details can lead to different types of fraud. During the current technological

advancements where cyber security has been a crucial issue affecting data safety, organizations need to establish deep learning systems through software engineering that shall replace their perimeter-based security solutions. Besides, organizations should be warned against the use of network-based security solutions whose security levels are relatively lower and can be easily compromised by various approaches by the attacker from where information and data can be accessed. As a result, organizations can reinforce the security of their systems by establishing and implementing ID/PSs, whose security level is high and are also specially designed to detect various types of attacks from where appropriate security concerns such as aborting the execution or cutting off the network connection can be done. Besides, IDPs involves a diverse range of techniques that include signature-based detection, anomaly-based detection, and stateful protocol analysis, each of which can operate independently or can be integrated to function as a single unit to bolster security against attackers trying to access credit card information or any other data in the organizational systems. The sensitivity associated with security of data, especially credit card details of customers, is an essential field that requires in-depth research to counter malicious access in the future. Besides, organizations needs to establish crucial and long-term projects aimed at enhancing the security of their systems and which should be evaluated at different development stages to ensure accuracy, effectiveness and high functionality. Besides, organizations, especially financial and software developing organizations, need to invest heavily financially to ensure that projects aimed at installing IDPs and IPS are not called off due to financial challenges that might arise along the process.

REFERENCES

[1] Ali, M. A., Azad, M. A., Centeno, M. P., Hao, F., & van Moorsel, A. (2019). Consumer-facing technology fraud: Economics, attack methods, and potential solutions. Future Generation Computer Systems, 100, 408-427. Arpteg, A., Brinne, B., Crnkovic-Friis, L., & Bosch, J. (2018, August). Software engineering challenges of deep learning. In 2018 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA) (pp. 50-59). IEEE.

[2] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. In 2018 10th international conference on cyber Conflict (CyCon) (pp. 371-390). IEEE.

[3] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419.

[4] Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Information Sciences, 479, 448-455.

[5] Jayanta, Y. (2013). Classification of Intrusion Detective and Prevention Systems. Available at https://www.researchgate.net/figure/Classification-of-intrusion-detection-and-prevention-systems_fig1_271070098. Accessed 20 April, 2022.

[6] Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. Expert Systems with Applications, 100, 234-245.

[7] Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. Information Management & Computer Security.

[8] Scarfone, K., & Mell, P. (2010). Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft) Recommendations of the National Institute of Standards and Technology. Available at https://csrc.nist.rip/library/alt-SP800-94r1-draft.pdf. Accessed 20 April, 2022.