ETHICAL HACKING USING AI AND ITS EFFECTS ON FINANCIAL MARKET

A REVIEW PAPER

[1]Shital Mahajan, [2]Dr. Shivangini Morya,
[1]Phd Scholar, [2]Associate Professor,
[1]Electronics and Telecommunication Engineering,
[1]SAGE University , Indore, India

Abstract : The recent trend of cyber attacks against critical infrastructure systems have necessitated that to examine the impact of such attacks on stock market. The question is arrives that 'How insider trading law addresses computer hackers who employ hacking in relation with the buy and sell of securities?' Current securities law is ill equipped to deal with such hackers because, unlike the typical defendants in insider trading cases, hackers owe no fiduciary duty to shareholders and no duty of confidentiality to insiders that provide material non public information. Hackers who trade on the basis of information they obtained through hacking do not fit either of these two categories. Hackers are corporate outsiders who owe no duty to shareholders and no duty to insiders who share information in order to trust

***Index Terms* – Hacking, Artificial Intelligence, Machine learning, stock market, Cyber Attacks, Cyber Security.**

I. INTRODUCTION

As public and private organizations migrate more of their critical functions to the Internet, criminals have more opportunity and incentive to gain access to sensitive information through the Web application. Thus the need of protecting the systems from the nuisance of hacking generated by the hackers is to promote the persons who will punch back the illegal attacks on our computer systems. So, to overcome from these major issues, ethical hackers or white hat hackers came into existence. "Ethical Hacking" which attempts to pro-actively increase security protection by identifying and patching known security vulnerabilities on systems owned by other parties. Ethical hackers may beta test unreleased software, stress test released software, and scan networks of computers for vulnerabilities. Ethical hacking can be defined as the practice of hacking without no malicious intention, rather evaluate target system with a hackers perspectives. Hacking is a process to bypass the security mechanisms of an information system or network. The main purpose of this study is to reveal the brief idea of the ethical hacking and its affairs with the corporate security [1]. Nowadays there are many techniques used by hackers in Ethical Hacking. But hacking using artificial intelligence is still rare.

Hacking is an activity in which, a person exploits the weakness in a system for self-profit or gratification. Ethical hacking is an identical activity which aims to find and rectify the weakness in a system. In the growing era of internet computer security is of utmost concern for the organizations and government. These organizations are using Internet in their wide variety of applications such as electronic commerce, marketing and database access. But at the same time, data and network security is a serious issue that has to be talked about. Thus to discuss the overview of hacking and how ethical hacking disturbs the security. Also the Ethical Hackers and Malicious Hackers are different from each other and playing their important roles in security. [2] This studied the different types of hacking with its phases. The hacking can also be categorized majorly in three categories such as white hat, black hat and grey hat hacking. We also presents a comparison of the hacking categories with different methods of penetration testing.

II. AI USED IN HACKING

Despite the differences between cyber security vs artificial intelligence, they combine to eliminate complexities and improve security. The three most significant characteristics of AI are its ability to learn, adapt, and generalize. Because of these characteristics, AI is required in ethical hacking activities. The main reason for this is that black hat hackers' strategies, tactics, and actions are constantly changing. As a result, white hackers must adapt to identify and address issues and vulnerabilities continuously.

Due to these hackers the most affected is banking and stock market sector, and which also show their effects on economy of the country. Given the successful cyber-attacks against high-profile financial institutions, the possibility of hackers disrupting individual shares or funds in the stock market is very real. There are different scenarios for widespread financial chaos and major loss caused by hackers. After targeting government and banking systems, cyber-attackers are now turned their focus on stock market. There has been increase in cyber attacks through new types of phishing scam where fraudsters are setting up fake websites that looks exactly same as the trading website of leading brokerages.

Hacking is convenient for criminals as there is no geographic barrier and cheap to perform. In addition, it is hard to identify the criminals behind the attack. Hence, it is expected that the number of hacker attacks will continue to increase and that the hackers will become more sophisticated in their methods [10].

.

III. LITERATURE REVIEW

There are many papers and articles and much more material is avaliable on this topic to discuss. So I choose some of them.

Firstly **C. Nagarani** has told about introduction of ‘Hacking’ and ‘Ethical Hacking’ he said ‘Hacking’ is not a modest process or categorization of instructions as many ponder. Hacking is a talent / skill / knowledge. Hacking is unlicensed use of computer and network resources. Computer hacking is the art of amending computer hardware and software to achieve an objective outside of the author’s unique determination. People who involve in computer hacking activities are called as hackers. Ethical hacking is also called as penetration testing or white-hat hacking. The knowledge of testing the system nodes and network for security susceptibilities and plugging the fleabags find before the bad guys get an opportunity to mishandle them. Ethical hacking and ethical hacker are terms used to define hacking performed by a company or individual to help identify prospective threats on a computer or network. An ethical hacker attempts to circumvent way past the system security and search for any feeble facts that could be ill-treated by malevolent hackers. This information is then used by the body to improve the system security, in an effort to abate or eradicate any probable attacks Ethical hacking is authorized. Ethical hacking is performed with the target’s authorization. The commitment of ethical hacking is to identify susceptibilities from a hacker’s viewpoint so systems security can be well enhanced. Ethical hacking can also ensure that vendors’ claims about the security of their products are legitimate [7]. He also shortly explained different phases of hacking and some techniques of hacking.

K.Bala Chowdappa , S.Subba Lakshmi , P.N.V.S.Pavan Kumar has also explained details about hacking phases and also techniques with types of hackers in their paper namely ‘Ethical Hacking Techniques with Penetration Testing’ and finally they siad that Hacking has both its benefits and risks. Hackers are very diverse. They may bankrupt a company or may protect the data, increasing the revenues for the company. The battle between the ethical or white hat hackers and the malicious or black hat hackers is a long war, which has no end. While ethical hackers help to understand the companies’ their security needs, the malicious hackers intrudes illegally and harm the network for their personal benefits. An Ethical and creative hacking is significant in network security, in order to ensure that the company’s information is well protected and secure. At the same time it allows the company to identify, and in turn, to take remedial measures to rectify the loopholes that exists in the security system, which may allow a malicious hacker to breach their security system. They help organizations to understand the present hidden problems in their servers and corporate network. The study also reveals that the valid users are the ethical hackers, till their intensions are clear otherwise they are a great threat, as they have the access to every piece of information of the organization, as compare to total and semi outsiders. Hacking is an important aspect of computer world. It deals with both sides of being good and bad. Ethical hacking plays a vital role in maintaining and saving a lot of secret information, whereas malicious hacking can destroy everything. What all depends is the intension of the hacker. It is almost impossible to fill a gap between ethical and malicious hacking as human mind cannot be conquered, but security measures can be tighten.[1]

Prabhat Kumar Sahu, and Biswamohan Acharya had said I their paper named as ‘A Review paper on Ethical Hacking’ that Ethical hacking technology spreads to diverse areas of life and in particular to every walks of the computer industry. The required to protect dominant data of the common should be communicate with the correct technology. Because of the smartness of hackers, ethical hacking arose as the latest and innovative computer technology. To protect their data, every small or large organization adopts this as the front layer of security. Understanding the general public's true intentions in these days is quite a difficult task, & it even more difficult to appreciate the motives of each ethical hacker entering vulnerable networks or systems.
They also explained about tools of hacking and types of Hackers as follows.

1.**White-hat**: A white-hat hacker, also known as the ethical hackers, is celebrity who has non-mischievous intent every time they breaks into security systems. Most white-hat hacker is safety specialist, often working with a company to track & enhance security weaknesses legally.
2.Black-hat: The ' black-hat ' hackers, sometimes referred to as a ' cracker, ' is celebrity who hack with malicious intent & without permission. The hackers typically want to prove her or his hacking skills & will perform a variety of cybercrimes, such as credit card fraud, identity theft and piracy. A black hat hacker is a person with detailed computer knowledge aimed at infringing or bypassing internet security.
3.Grey-hat: As the color suggests, somewhere between white-hat & black-hat hackers is a ' grey-hat ' hacker, as he or she possesses both characteristics. For example, in search of compromised systems, some grey-hat hackers will roam in the Internet; like the white-hat hackers, the targeted company will be aware of any vulnerability & will patch them, but like the grey-hat hacker, the black-hat hacker will hack without permission.
4. Blue-hat: Independent specialist companies for computer security are employed to check a program for vulnerabilities before it is released, finding weak links that can be removed. Blue hat is also affiliated with Microsoft's annual security convention where Microsoft engineers & hackers are able to communicate freely. Blue hat hackers are someone outside of the consultancy firm of computer security who tests a system before it is launched, looking for exploits to be closed. The Blue Hat Hacker is also referring to Microsoft's security executive to execute arbitrary code in Windows. The word was also connected with Microsoft's annual security convention, the unofficial names associated with Microsoft employee badges from the blue color.
5. Elite Hacker: These types of hackers that have prominence as the ' best in the business ' & are regarded as the innovators & experts. The invented language called ' Leets peak' was used by elite hackers to shield their pages from searching engines. A language meant that few letters were replaced in a word by the numerical similarity or other similar letters. The hacker is a common phase used to describe to a person who covertly gains access for the purpose of earning money to systems and networks. However, some practice the creative art of hacking because they get a certain amount of excitement from the test they are put into.[9]

Aman Gupta and **Abhineet Anand** had published their opinions in the paper as ‘Ethical Hacking and Hacking Attacks’. They told about the hacking techniques on different operating system step by step as follows:
The Code Of Conduct Of An Ethical Hacker: -1. Identifying and determining the confidentiality and privacy of the data of any organization before hacking and should not violate any rule and regulations.
2. Before and after the hacking maintaining the transparency with the client or owner of the organization.
3. The intensions of an ethical hacker must be very clear, that not to harm the client or organization.
4. Working within the limits set by the client or the organization, do not go beyond them.
5. After the hacking do not disclose the private or confidential findings during the hacking with others.[3]

Kenneth Geisler II: This paper explores how insider trading law addresses computer hackers who employ cyber attacks in connection with the purchase or sale of securities. Current securities law is ill-equipped to deal with such hackers because, unlike the typical defendants in insider trading cases, hackers owe no fiduciary duty to shareholders and no duty of confidentiality to insiders that provide material non-public information. Hackers who trade on the basis of information they obtained through hacking do not fit in either of these two categories. Hackers are corporate outsiders who owe no duty to shareholders and no duty to insiders who share information in trust. Unlike a misappropriator who exploits a relationship of trust in order to gain valuable information, hackers rely on their technical knowhow to obtain the information. In other words, “Although the hacker’s advantage was [also] unfair, he garnered it not through privilege or special connections but through the much rarer combination of superior technologies, risk-taking, and criminal bravado.” This paper explores the challenge in holding computer hackers liable for insider trading. It adds to the existing literature by arguing that even if the courts ultimately adopt the SEC’s theory of insider trading, there would still remain the potential for innovative hackers to avoid liability. [2] Actually we have to focus on the things of this paper that how hackers can be used his techquenics for spoil stock market or for his own profit from the stock market.

Onur Kemal Tosun: In their study they explain, how financial markets respond to unexpected fraudulent corporate security breaches both in the short term and in the long term. In particular, he investigate how daily excess returns, market activity and bid-ask spreads react in the days around the public disclosure of hacking events. In the short term, the results show that, while excess returns drop the day after the breach announcement, both the traded volume and the bid-ask spread significantly increase at the announcement date. In addition, a signed volume measure, calculated as the product of realized returns, and raw traded volume suggest that short-term market activity is primarily driven by a selloff of shares. The findings show that such changes in market activity can be due to increasing investors’ attention, proxied by search frequency on Google, at the public disclosure of the security breach. Further results indicate that security breaches and subsequent trading lead to transmission of confidential information about target firms into prices that can cause further damage to those companies.

In the longer term, the empirical analysis shows that, while operating performance is not significantly affected up to five years after the event, firms’ policies significantly incorporate security breaches by investing more in the existing management. To summarize, the results are consistent with the idea that a data breach constitutes an exogenous negative shock to a firm's reputation and thus, future growth prospects.[11]

As Mr Andrew Lohn says: Artificial intelligence is vulnerable to cyber attacks. Machine learning systems—the core of modern AI—are rife with vulnerabilities. Attack code to exploit these vulnerabilities has already proliferated widely while defensive techniques are limited and struggling to keep up. Machine learning vulnerabilities permit hackers to manipulate the machine learning systems' integrity (causing them to make mistakes), confidentiality (causing them to leak information), and availability (causing them to cease functioning). These vulnerabilities create the potential for new types of privacy risks, systemic injustices such as built-in bias, and even physical harms. Developers of machine learning systems—especially in a national security context—will have to learn how to manage the inevitable risks associated with those systems. They should expect that adversaries will be adept at finding and exploiting weaknesses. Policymakers must make decisions about when machine learning systems can be safely deployed and when the risks are too great. Attacks on machine learning systems differ from traditional hacking exploits and therefore require new protections and responses. For example, machine learning vulnerabilities often cannot be patched the way traditional software can, leaving enduring holes for attackers to exploit. Even worse, some of these vulnerabilities require little or no access to the victim's system or network, providing increased opportunity for attackers and less ability for defenders to detect and protect themselves against attack

Machine learning introduces new risks: Using machine learning means accepting new vulnerabilities. This is especially true in Center for Security and Emerging Technology the context of national security, but also in critical infrastructure, and even in the private sector. However, this does not mean machine learning should be prohibited. Rather, it is incumbent upon policymakers to understand the risks in each case and decide whether they are outweighed by the benefits.

New defenses may only offer short-term advantage: Attackers and defenders of machine learning systems are locked in a rapidly evolving cat-and-mouse game. Defencer are lake behind to stop the attacks due to latest attackers skills.

Robustness to attack is most likely to come from system-level defenses: Given the advantages that attackers have, for machine learning systems to function in high-stakes environments, they must be built in with greater resilience than is often the case today.

Machine learning has already transformed many aspects of daily life, and it is easy to see all that the technology can do. It likewise offers the allure of reshaping many aspects of national security, from intelligence analysis to weapons systems and more. It can be hard, however, to perceive machine learning's limitations, especially those—like its susceptibility to hacking—that are most likely to emerge in highly contested environments. To better understand what the technology can and cannot do, this primer introduces the subject of machine learning cyber security in a detailed but non-technical way. It provides an entry point to the concepts and vocabulary needed to engage the many important issues that arise and helps policymakers begin the critical work of securing vital systems from malicious attacks.[5]

Mr. Marc Ruef in their published paper says that : Artificial intelligence (AI) is playing an ever greater role in our technocratic society. The automated collection and processing of data is making it possible to reproduce intelligent or even human-like behavior. Because the method has taken on such a central role, it is creating some major risks. This article discusses the extent to which AI can be hacked. The discussion presented here applies to both strong and weak AI applications in equal measure. In both cases, input is collected and processed before an appropriate response is produced. It doesn't matter whether the system is designed for classic image recognition, a voice assistant on a smartphone, or a fully automated combat robot. The goal is the same: to interfere with the intended process. This kind of disruption is any deviation from the ideal behavior (https://www.computec.ch/projekte/tractatus/? s=tractatus) or, in other words, the goal, expected outcome or normally observed outcome during the development, implementation and use of an AI application. Image recognition might be tricked into returning incorrect results; illogical dialogs might be prompted with a voice assistant; or the fundamental behaviors of a combat robot might be deliberately overridden.[8]

Kim Hartmann and Christoph Steup said in their paper that, Over the past decades, modern computer networks, infrastructures and digital devices have grown in both complexity and interconnectivity. Cyber security personnel protecting these assets have been confronted with increasing attack surfaces and advancing attack patterns. In order to manage this, cyber defense methods began to rely on automation and (artificial) intelligence supporting the work of humans. However, machine learning (ML) and artificial intelligence (AI) supported methods have not only been integrated in network monitoring and endpoint security products but are almost omnipresent in any application involving constant monitoring, complex or large volumes of data. Intelligent IDS, automated cyber defense, network monitoring and surveillance as well as secure software development and orchestration are all examples of assets that are reliant on ML and automation. These applications are of considerable interest to malicious actors due to their importance to society. we report on the state of the art of attack patterns directed against AI and ML methods. We derive and discuss the attack surface of prominent learning mechanisms utilised in AI systems.

In their paper they start by giving a brief introduction to selected AI and ML methods currently deployed. Then they report on state of the art attack patterns directed against these systems and how it must be expected that these systems will become prominent targets over the next decade. They derive and discuss how attack surfaces may be modeled for AI systems. they apply the previously derived attack surface model to AI systems utilizing the different methods to compare their susceptibility to attacks. They conclude with an analysis of the implications of AI and ML attacks for the next generation of cyber conflicts and recent mitigation strategy attempts.[4]

Matti Mantere said in her paper published in IEEE Journals that False information spread through on-line social media and various news outlets can cause significant fluctuations in equity markets around the world. This fluctuation is partially independent of the initial cause of the chain of events that lead to an inaccurate piece of information becoming a widespread rumor. In this paper a method for manipulating stock markets is presented together with a hypothetical case study. The method leverages the way that even unverified information spreads through social and other on-line media. This is done by intentional dissemination of a made-to-order rumor while simultaneously covertly launching cyberattacks as a catalyst to this process. The intention of this type of activity can is to affect the targeted equity markets for the financial gain of the perpetrators. Through a presentation of a hypothetical case study we argue that the method presented is a viable method for producing illicit gains for criminal groups, and some forms of it might already be in use by some actors.

Introduction to Stock Market Dynamics and Cybersecurity

The stock market operates as a cornerstone of modern financial systems, reflecting a nation's economic health and global market trends. The efficiency and security of stock exchanges are crucial for sustaining investor trust. In the digital era, exchanges rely heavily on technology to process millions of trades daily. However, this dependence on digital infrastructure makes them vulnerable to cyberattacks, a rising threat in recent years. Cybersecurity in financial systems has been extensively studied, highlighting the risks and consequences of breaches in stock exchanges.

Hacking and Its Evolution in Financial Markets

The integration of technology into financial markets has ushered in new methods of fraud, manipulation, and hacking. A study by Khan et al. (2020) emphasized how hackers exploit vulnerabilities in trading algorithms and networks. High-profile breaches, such as the NASDAQ hacking in 2010, underline the potential havoc cyber intrusions can wreak. Though direct manipulation of trades in such cases remains rare, the very exposure of vulnerabilities shakes investor confidence and market stability.

The Role of Artificial Intelligence in Stock Market Operations

AI's role in financial markets is twofold: it enhances efficiency and creates new avenues for exploitation. Research by Patel and Singh (2021) showed that AI-based algorithms enable faster trading decisions and pattern recognition but are not immune to cybersecurity threats. Hackers can use AI to craft sophisticated attacks or manipulate trading algorithms, leading to unintended ripple effects across markets.

Indian Stock Market and Cybersecurity Challenges

India's stock exchanges, such as the NSE and BSE, are significant players in global markets. However, they are not immune to the challenges posed by cyber threats. Studies by Sharma and Verma (2022) revealed that while Indian exchanges have invested heavily in cybersecurity infrastructure, incidents of data breaches and irregular trading activity persist. SEBI's warning in 2023 about cybersecurity underscored the urgent need to address these issues, as even minor breaches could trigger massive market disruptions.

Impact of Global Markets on Indian Stock Exchanges
Global financial markets are interconnected, and fluctuations in indices like the Dow Jones, NASDAQ, and Nikkei influence Indian markets. A study by Mukherjee and Reddy (2019) demonstrated that global indices often serve as leading indicators for Indian market movements. In cases of cybersecurity breaches in global exchanges, the ripple effects are evident in Indian markets, where volatility increases due to uncertainty.

Cyber attacks in a more technical sense are not discussed in this paper, nevertheless research done on cyber-attacks is very important for this paper. Books such as “the web application of hackers handbook” include detailed information on how to break web applications and exploit flaws discovered in them. In this paper the detailed approach is not used. This paper is more about the general method of leveraging the stock market effects of the spread of misinformation with usage of targeted cyber-attacks. Also, general market manipulation is not discussed at great detail in this paper. The attack itself can be varied greatly. The cyber-attack part might be emphasized more, or less as the spread of misinformation through the social media channels. The proportions of the attack itself can vary greatly, which should be taken into account when attempting to detect these types of manipulative attacks. Detection and protection against the type of an attack as described in this paper requires more research and active discussion on the vulnerabilities inherent in the current system which are exacerbated by the continuous flow of unverified information from uncertain sources.[6]

The economical specifics such as the ideal volatility, actual derivatives to be used and such are left out of the scope of this paper. The author wishes to stress, that activity as described in this paper is highly illegal in many, if not all, jurisdictions around the world and must not be tested in real settings. It must also be noted that the author is a cyber security researcher, not an economist, and would like to apologize for any mistakes or confusion in the financial terminology.

IV RESULTS

The literature reviewed provides comprehensive insights into hacking, ethical hacking, and their implications for cybersecurity and financial markets. Here are the key results derived from the reviewed works:

1. **Distinction Between Ethical and Malicious Hacking**
   Several studies, such as those by C. Nagarani and K. Bala Chowdappa et al., underscore the dual nature of hacking. Ethical hacking emerges as a proactive tool for identifying vulnerabilities and safeguarding systems, whereas malicious hacking exploits these vulnerabilities for personal or financial gain. The clear delineation between ethical ("white-hat") and malicious ("black-hat") hackers helps organizations understand the necessity of ethical practices to protect sensitive data and maintain system integrity.

2. **Growing Importance of Ethical Hacking in Network Security**
   The research highlights the critical role of ethical hacking in identifying security loopholes and preempting attacks. Ethical hackers provide organizations with a hacker’s perspective, enabling them to enhance security measures. This proactive approach helps mitigate risks, ensuring the stability of critical systems such as corporate networks and financial server.

3. **Impact of Hacking on Financial Market**
   Studies, such as those by Onur Kemal Tosun and Matti Mantere, provide evidence of how hacking and cyberattacks destabilize financial markets. Security breaches lead to immediate impacts, including a decline in stock returns and increased volatility. In the long term, affected firms incorporate lessons learned by strengthening policies and investing in cybersecurity. These findings highlight the interconnectedness of cybersecurity and financial stability.

4. **Legal and Regulatory Gaps in Addressing Financial Hacking**
   Kenneth Geisler II's work reveals significant gaps in current insider trading laws for addressing cyberattacks. Hackers, as corporate outsiders, do not fit traditional definitions of fiduciary relationships, making it difficult to prosecute them effectively. This underscores the urgency of updating legal frameworks to address the evolving nature of hacking in financial systems.

5. **Vulnerabilities of Artificial Intelligence Systems**
   Studies by Andrew Lohn and Marc Ruef demonstrate the vulnerabilities of AI systems to cyberattacks. AI's reliance on machine learning introduces risks that cannot be easily patched, leaving systems open to manipulation. These vulnerabilities have far-reaching implications, particularly in high-stakes environments like national security and financial systems.

6. **Role of Misinformation and Cyberattacks in Stock Manipulation**
   Matti Mantere's research reveals how false information spread through social media, combined with cyberattacks, can manipulate stock markets. This underscores the increasing sophistication of hacking techniques, where social engineering complements technical attacks to disrupt markets.

7. **Challenges in Bridging the Gap Between Ethical and Malicious Hacking**
   The literature highlights the challenge of fully bridging the gap between ethical and malicious hacking. Intent remains a critical factor, with ethical hacking's legitimacy depending on clear motivations and strict adherence to boundaries. The inability to predict human intent entirely means that security measures must continuously evolve to address potential threats.

IV. Conclusion

By studying all the related papers and articles I decided that the whole world is moving towards the enhancement of technology, and more and more digitization of the real world processes, with this the risk of security increases. This described the working of malicious hackers or crackers on one hand who tries to illegally break into the security and on the other hand white hat hackers or ethical hackers, who tries to maintain the security. As in the computer system, hacking plays a vital role as it deals with both sides of being good or bad. Further, the types, working, and various attacks performed by the hackers. It must be said that Ethical Hacking is a tool which when properly utilized can help in better understanding of the computer systems and improving the security techniques as well.

Nowadays advanced development in the field of software and also in electronics is happening Artificial intelligence is one of them example. So sites are now been secured with using AI, and so hackers are also not stay backward in the same. They are also findings new techniques of hacking AI too.

Stock market and banking sector are the main aim of hackers. Untill we do not know the ways hackers used we cannot provide security to our economy. We find an average negative stock market reaction. Moreover, we find that the stock prices do not fully recover within the following ten days, indicating that shareholder value is at risk. When investigating the role of consumers, we find that when many client's records are exposed in the hack, the stock market reaction is stronger. This may be because investors expect that the consumers will use their market power to punish the companies that have been hacked, and that this will decrease the net value of the company. More surprisingly, we find no statistically significant impact when the data exposed in the hack is sensitive to the customers.

REFERENCES

[1] K. B. Chowdappa, S. S. Lakshmi and P. P. Kumar, ”Ethical Hacking Techniques with Penetration Testing” *(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) ,* (2014)*, 3389-3393.*

[2] K. Geisler*, "*Hacking wall street: Reconceptualizing Insider Trading Law for Computer Hacking and Trading Scheme*". https://ssrn.com/abstract=3221987* 2019.

[3] A. Gupta, and A. Anand, "Ethical Hacking and Hacking Attacks" *International Journal Of Engineering And Computer Science* vol 10. (2017).

[4] K. Hartmann, and C. Steup, "Hacking the AI - the Next Generation of Hijacked Systems". *IEEE , 12th International Conference on Cyber Conflict,* (2020).

[5] A. J. Lohn, "Hacking Ai A Primer For Policymakers On Machine Learning Cybersecurity*", Center for Security and Emerging Technology.* (2020).

[6] M. Mantere, "Stock Market Manipulation Using Cyber Attacks Together With Misinformation Disseinated Through Social Media*", IEEE computer society,*pp 950-54*SocialCom/PASSAT/BigData/EconCom/BioMedCom* (2013).

[7] C. Nagarani, "Ethical Hacking and Its Value to Security", *Gobal journal of research Analysis*(2015).

[8] M. Ruef, " Hacking Artificial Intelligence – Influencing and Cases of Manipulation". *ResearchGate* (2020, january).

[9] P. K. Sahu, and B. Acharya, "A review paper on Ethical Hacking", *International Journal of Advanced Research in Engineering and Technology (IJARET)* , vol 6. (2020).

[10] E. K. Jansen, S. M. Stavik ,"What the Hack?An Empirical Analysis of the Stock Market Reactions to Hacking". *Norwegian School of Economics , Bergen*, (2020).

[11] O. K. Tosun, "Cyber Attacks and Stock Market Activity". (2020).

[12] https://www.computec.ch/projekte/tractatus/? s=tractatus.

[13] A. Gupta and A. Anand, "Ethical Hacking and Hacking Attacks: A Comprehensive Guide," in *International Journal of Information Security Research*, vol. 11, no. 3, pp. 89-98, Sept. 2021.

[14] M. Green and D. McDonald, "Security Breaches and Financial Market Reactions," in *Journal of Cyber Economics*, vol. 8, no. 2, pp. 134-145, June 2020.

[15] H. Nguyen and P. Patel, "AI Vulnerabilities and Cybersecurity Measures," in *ACM Transactions on Cybersecurity and Privacy*, vol. 14, no. 1, pp. 77-93, Jan. 2022.

[16] T. Kamran and R. Stevenson, "Exploring Insider Trading via Cyber Exploits," in *Cyber Law and Policy Review*, vol. 19, no. 4, pp. 256-265, Oct. 2021.

[17] J. Turner, "Market Dynamics After Cyber Attacks: A Quantitative Study," in *Journal of Financial Technology and Analytics*, vol. 9, no. 3, pp. 191-203, Aug. 2022.

[18] F. Scott, "Hacking AI: Challenges in Machine Learning Security," in *Proceedings of the 12th International Conference on AI Security*, London, UK, pp. 342-350, July 2021.

[19] E. Kim and Y. Zhou, "Mitigating AI Exploits in Financial Systems," in *IEEE Security and Privacy Magazine*, vol. 20, no. 2, pp. 59-68, Mar. 2023.

[20] S. Lee and J. Park, "Ethical Hacking in Practice: Tools and Techniques," in *IEEE Transactions on Information Forensics and Security*, vol. 18, no. 5, pp. 1123-1135, May 2023.

[21] Chan and M. Wilson, "The Role of AI in Mitigating Cyber Threats," in *Cyber Defense Review*, vol. 7, no. 3, pp. 203-214, Sept. 2021.

[22] P. Carter, "Data Breaches and Market Volatility: Evidence from Case Studies," in *International Journal of Financial Studies*, vol. 13, no. 2, pp. 345-358, Apr. 2023.