البنك المركزى المصرى
المعهد المصرفى المصرى

المركز الإعلامي العربي

المركز الإعلامي العربي يطلق

المسابقة البحثية

بالتعاون مع المعهد المصرفي المصري

لعام ٢٠٢٤

الأبحاث الفائزة بالمسابقة البحثية للمركز الإعلامي العربي
بالتعاون مع المعهد المصرفي المصري لعام 2024
حول موضوع
" استخدام الذكاء الاصطناعي في تعزيز الأمن السيبراني بالبنوك"

الفائزة بالمركز الأول

الأستاذة / سارة طارق محمود

البنك الأهلي المصري

Artificial intelligence in enhancing bank's Cyber security

Introduction

According to Network Readiness Index 2023for Egypt; Egypt ranked 81 where cybersecurity ranked 30 with 95.4 score, The online access to financial account is 125 with score of 3.38 (networkreadinessindex, 2023).

AI is used in Investigation, Identification, Reporting and Research, Where AI investigate can investigate the pattern from hackers and the users that were infected by tracking the URL's Domain to the IP Address of the source user, AI can investigate the action of users that seems unconnected using Machine Learning (ML)to identify the patterns that might seem unrelated to the human beings for example Deutsche bank uses Alpha-Dig Platform to subtract news from the media , the Social Media and Articles generating risk profile for the country , then the Alpha-Dig platform uses Wikipedia to learn as it's data is readable using Z-scoring statistical method it generates political reports situation (Kaya, 2019).

AI has become essential to prevent attacks and enhance cybersecurity in banking sectors for Example Qatar bank uses IBM Safer payment service as all systems of IBM 100% contains AI that helps analyzing fraudulent patterns , alerting for fraud threats and offer counter measures especially in credit card fraud also AI is used in the KYC process in Qatar bank *(Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges, 2022)*.

In the recent years cyber-attacks on the banks have increased from credit card fraud, money laundry and a lot more which takes us to the first topic.

Cyber security threats

Around70% of capital market ‘s CEO and banks’ CEO consider cyber-security a threat to their development where such threats can cause a loss cost 360$billion a year where financial institutions are 300 times more effected than business institution by security events *(A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking system, 2022).*

Cyber-attacks threats can cause wither direct or indirect loss for the financial institutions where the direct losses come from actual money loss due to fraud and data breach while the indirect losses come from poor public relation and dissatisfied customers , AI itself can be a major cyber-security threat where adversarial machine learning ML feeding a trained system a specific inputs to influence the outputs as Generative adversarial network (GAN) ML configuration used to find other ML system output errors ,the artificial intelligence improved in creating more advance content that convincedly true “deep fake” *(Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges, 2022, p. 5)*.

Types of cybersecurity threats

1. Phishing attacks: cybersecurity attackers use phishing emails where they send emails that seem from the organization to trick the users inside the organization in order to get access to sensitive information from passwords and access to systems that can’t be hacked by them *(Almutairi2, 2023)*.

2. Ransomware: demanding payment data to get access to credit and debit cards in order to cause financial damage *(Almutairi2, 2023).*
3. DDoS Attacks (Distributed Denial of Service): overwhelming banking's network to cause disturbance in the operations and traffic in order to weaken the Defense system, AI is very advanced tool it will help monitoring data and more network platforms than the human capability of monitoring large traffic transactions yet it can't make the final decision.
4. Data Breaches & Insider Threats: using hacking or unauthorized access to data and customer's sensitive information either using hacking techniques or Employees misusing their positions to their own interest.
5. Third party vulnerabilities: AI is very expensive software which needs to be updated continuously and in case of failure system recovery will be time consuming and expensive (Venkata Siva Prakash Nimmagadda, 2021)so using third party will be a lower cost alternative yet with a sensitive data such as banks it will be riskier.

AI can be used to imprison audio or a video, tailor a phishing email attack data or to subtract data where it was reported that cybercrimes losses globally has reached 400$ billion at the US *(Almutairi2, 2023).*

Preventing Cyber security threats

Double authentication process is very important to prevent fraud to protect the banking customers financial accounts by using both password + physical or soft token or OTP in addition to Facial recognition or finger print while monitoring transaction to detect unfamiliar pattern or suspicious behavior

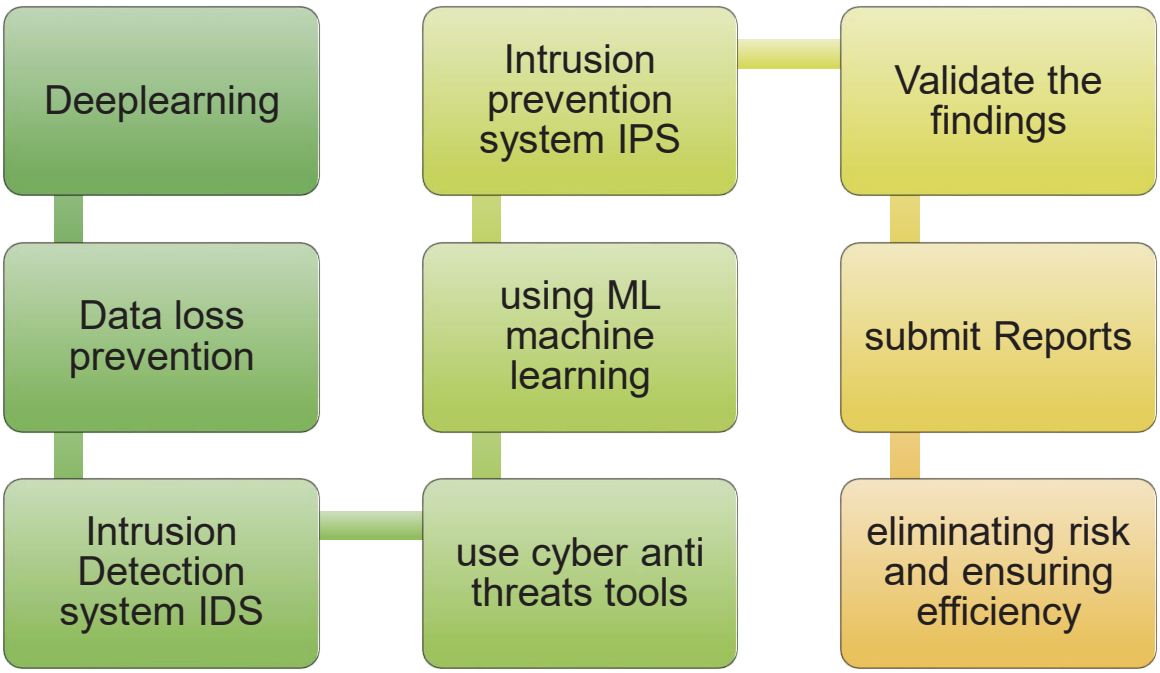
(Layla Abdel-Rahman Aziz, The Role Artificial Intelligence in Modern Banking: An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance, 2023).

Cybersecurity threats also can be avoided by using cloud computing technology where customers can access the technology without accessing to the major banking system, this technology is lower in capital and IT-services cost where the data is provided from the same cloud service provider where cloud technology is used as a conversion technology "as a cloud" *(A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking system, 2022).*

AI will face challenges regarding cybersecurity where it has to ensure accuracy of data collection along with the quality of data also human resistance will be a challenge because of fear of change and the fear of unemployment *(Venkata Siva Prakash Nimmagadda, 2021).Also AI can show biasness in Data, Algorithmic and human bias.*

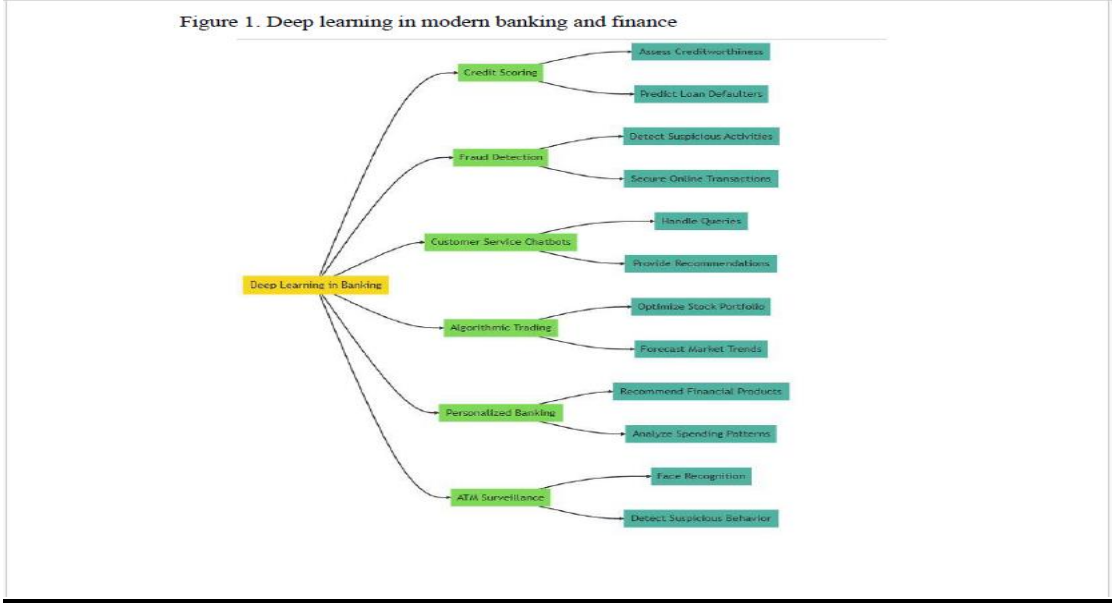
Although AI role is important in password-based attacks such as (RNN) Recurrent Neural Network and (GAN) Generative adversarial Network but it was reported that QATAR Bank used AI to detect such attacks but the traditional methods were more effective in preventing the attacks (Locking the accounts- Refreshing passwords -Forcing Captchas- mailing customers alerting multiple login trials failure) *(Almutairi2, 2023).*

Tools used by the AI



(A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking system, 2022).

I. Deep learning



(Layla Abdel-Rahman Aziz, The Role Artificial Intelligence in Modern Banking An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance).

II. Data loss prevention: where AI analysis big data to detect any cyber threats that might carried for example through emails and will cause the company to loss sensitive data.

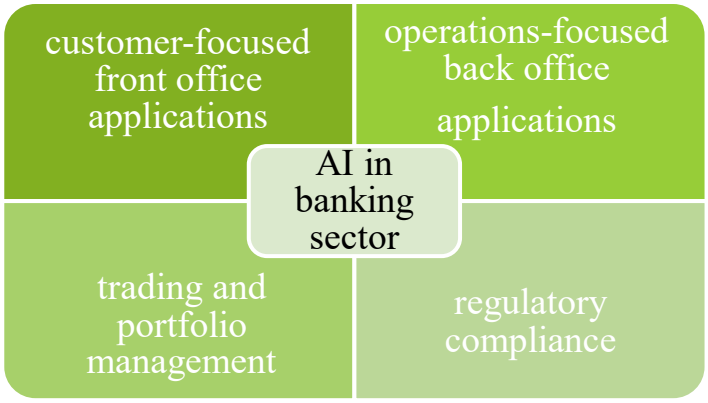
III. Intrusion Detection system IDS: to detect untrusted source and alert for traffic or Anomaly moves that might cause attack on system network

IV. Intrusion prevention system IPS: using ML machine learning tools to detect suspicious patterns through behavioral analysis and threat prediction, AI classify the patterns if they are harm or not using the cyber-attacks analysis tools entered in it.

V. Validate the findings, submit reports of the whole process eliminating risk and ensuring efficiency.

Future Artificial Intelligence Uses

Artificial intelligence usages can be divided into four main categories



(Kaya, 2019).

Using AI can help in enhancing efficiency by automation the routine tasks, reducing human errors, Also AI can mitigate risk by detecting fraud attempts and money laundry and financial crimes, AI generate reports on customer behavior, market trends and risk profiles helping to better decision making .AI can create competitive advantage for early adaptors *(Venkata Siva Prakash Nimmagadda, 2021).*

I. AI use Knowledge based system where it anticipates and report as an expert based on information and decision-making methodology entered through the AI before.
II. AI analysis customer behavior and provide personalized experience to create a strong relationship with the customers.
III. Using chatbots can be used in banking sectors to provide 24hr service which is fast and efficient answering most common questions increasing customer satisfaction and lower indirect losses *(Benediktus Rolando1, 2024).*
IV. AI have an important role in credit scoring where Its analysis the data and give accurate assessment and many financial institutions use AI for

fraud detection where AI can investigate and detect suspicious patterns and also study selling patterns and customer activities to increase sales and cross-selling efficiently.

V. Self-regulation tool that is in AI permits data regulation decreasing cost, securing ROL ensuring service accuracy and speed.

VI. AI improves machine driven procedures in banking sector increasing accuracy and security. *(A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking system, 2022).*

VII. deep-learning optical character recognition (OCR) for scanning documents which helps in sorting and tagging documents *(Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges, 2022)*. This is used in visualizing learning legal documents to reports by extracting important clauses from legal documents and learn from them to create more accurate reports *(Kaya, 2019).*

VIII. Some applications for AI as (Visual assistance for customers giving a personalized experience- Credit reporting with a credit risk management and loan losses predictions that alleging with the institution risk mitigation polices -Anti money laundry and fraud attempts tracking and also investment management *(Karan Sambre,Deepanshu Joshi, 2022)*.

IX. Combining Blockchains with AI; Blockchain is a ledger technology which is distributed to offer security of information and risk mitigation by scattering data using AI with blockchain it will help to generate coded contracts that align with compliances, enforcing regulatory requirements changing the whole process into Automated process where AI can observe blockchain data to identify suspicious activities

on accounts, prevent fraud and generate compliance reports using blockchains *(Almutairi2, 2023)*.

Conceptual model

Adopting the model of Wael Sh. Basri and Abdullah Almutairi in their article"

Enhancing Financial Self-efficacy through Artificial Intelligence (AI) in Banking Sector "**to** investigate AI applications using the trust in AI as a mediating variable while bank transparency as a moderating variable where they sat the following hypnosis

H1: Trust in AI technology mediates the relationship between AI adoption in fraud detection and financial self-efficacy

H2: Trust in AI technology mediates the relationship between Digital Assistant AI in transaction monitoring and financial self-efficacy

H3: Trust in AI technology mediates the relationship between Facial Recognition AI in transaction monitoring and financial self-efficacy

H4: Trust in AI technology mediates the relationship between Chatbot AI in transaction monitoring and financial self-efficacy

H5: Trust in AI technology mediates the relationship between employee AI understanding and financial self-efficacy

H6: Bank transparency moderates the relationship between understanding AI and trust in AI technology

H7: Bank transparency moderates the relationship between AI adoption in fraud detection and trust in AI technology

H8: Bank transparency moderates the relationship between Digital Assistant AI in transaction monitoring and trust in AI technology

H9: Bank transparency moderates the relationship between Facial Recognition AI in transaction monitoring and trust in AI technology

H10: Bank transparency moderates the relationship between Chatbot AI in transaction monitoring and trust in AI technology

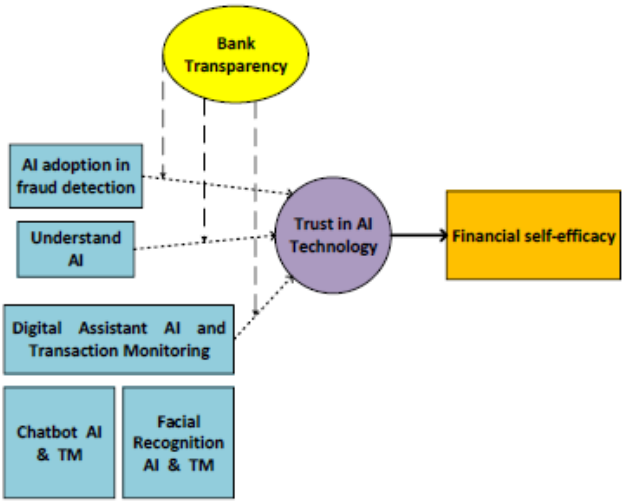


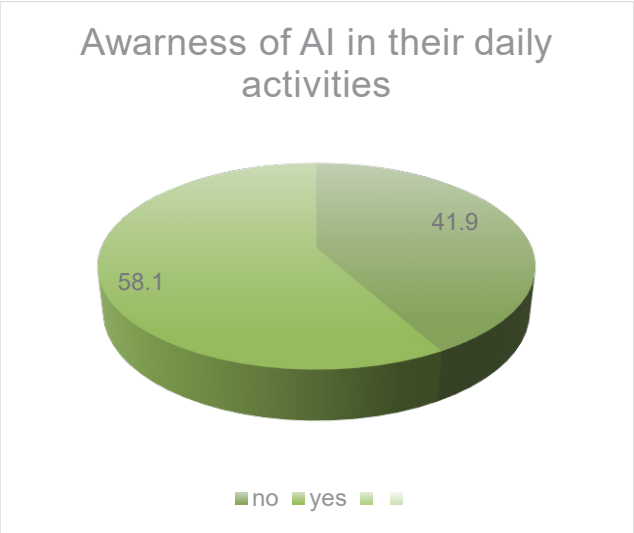
Figure 1: Conceptual Framework.

(Almutairi2, 2023)

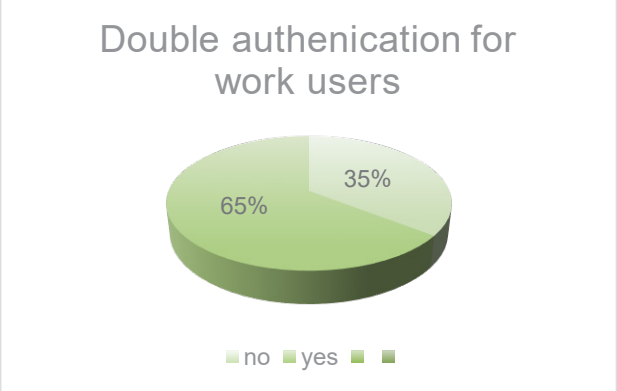
A questioner was conducted of a total 11 questions in the national bank of Egypt where the sample were 31 people … the questions were as following

- Age group?
- Where you work (front office customer focused- back-office compliance – investment and finance – back-office operations)
- Are you aware of applications that is using AI?
- Are you aware of applications that is using AI in your bank system?
- Are you aware of cyber-security threats?
- Are you aware of the counter majors of cyber-security threats?
- Do you use AI in your daily activities?
- Do you prefer using double authentication to login to your bank work user?
- Do you use biometric login to your Financial Account?
- Do you feel using AI will be challenging for you in work?
- Do you feel AI will replace humans in banking sector?

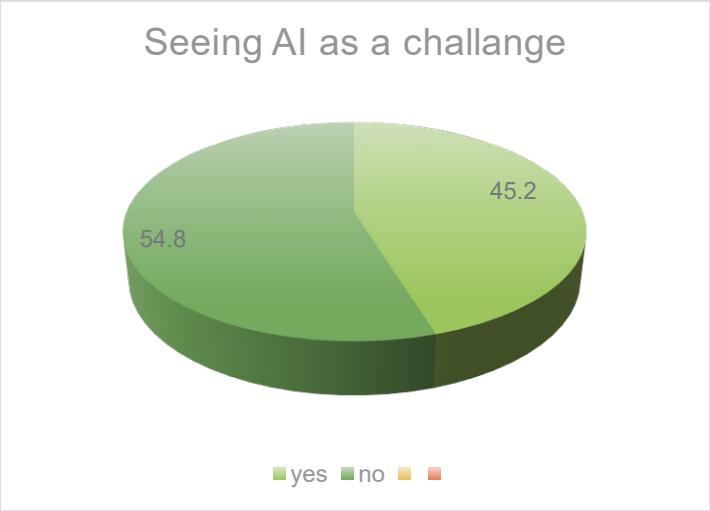
It was found that :58.1% from 31 replays said that they use AI in their daily activities yet 41.9% said no which means either they don't know that AI is in all mobile phone application.



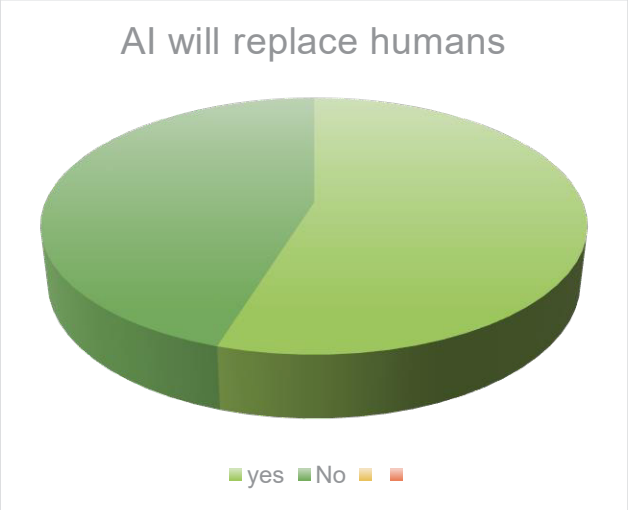
35.5% answered that they don't prefer double authentication when using their work users yet it was found that 80.6% prefer to use biometric access when they open their online financial accounts.



45.2% sees that AI will be challenging for them to use at work while 54.8% sees otherwise which means people need more training and more courses to feel secure about using AI.



54.8% sees AI will replace humans at work in banking industry while the re rest sees no will be assisting only



Recommendations

- **Data:** Data quality is important for AI in order to give accuracy and protecting these data must be priorities to ensure the efficiency of AI, so forming teams in Banking sectors where Data is reviewed before using it as AI and setting error standards so when the process is automated AI can define the error and the percentage and filter the

inaccurate data itself. Example: Legal teams enter legal documents and review the legal documents and scan them if there was an perish of government law highlight the perish enter the data of the law and the risk factors for the organization it might cause the expected loss for the bank.

- **Start small:** Begin with applying AI in some applications to reduce the fear of using AI in employees and customers and to spread the awareness and to test AI system that was built not by a third part rather by the organization efficiency. Example: using fingerprint in banking system with (Disabled people – illiterate people – or in some transactions like transferring between customer accounts) along with the signature in the banking process until reaching efficiency then allow either choosing signature of fingerprint to be used in banks.
- **Encourage Data culture:** Either by clouding using AI, or combining blockchains used like in CRM systems with AI or centralize the Data to make it easier for the AI. Example using uploading CRM -KYC to the AI system to detect money laundry fraud or unusual activities on customers' accounts.
- **Discuses ethical considerations:** training for the employees open discussions.
- **Engage Regulatory authority**
- **Invest in Talents resources:** Train IT, send scholarships outside Egypt to learn from top countries in AI so financial organizations don't need to use third parties to build AI systems and maintain them.
- **Build metrices that ensure fairness and prevent biases**
- **Bias detection and mitigation techniques**

- **monitoring and evaluation:** there must be a continuously monitoring an evaluation of data and reports of AI as the financial sectors in banks is dynamic so we can't depend on AI as a final decision maker.
- **Transparency and explainability:** there must be always explanation the data inputs and outputs of AI and the decision-making reasons.
- **Data privacy and security**
- **Model Risk management**
- **Liability and Accountability:** there must be a professional department where it updates the inputs, monitor Ai performance and outputs ensuring credibility and reporting problems and create solutions.

References

A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking system. (2022, Septmber 22).

Almutairi2, W. S. (2023, July 2). Enhancing Financial Self-efficacy through Artificial Intelligence (AI) in Banking Sector. *International Journal of Cyber Criminology*.

Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges. (2022, August 23).

Benediktus Rolando1, H. M. (2024). Application of Artificial Intelligence Based Risk Management in Banking: A Systematic Literature Review.

Karan Sambre,Deepanshu Joshi. (2022, December). Analyzing the impact of Artificial Intelligence(AI) in the Finance and Banking sector.

Kaya, O. (2019, june 4). Artificial intelligence in banking A lever for profitability with limited implementation to date. p. 6.

Layla Abdel-Rahman Aziz, Y. A. (2023). The Role Artificial Intelligence in Modern Banking: An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance. p. 4.

Layla Abdel-Rahman Aziz, Y. A. (n.d.). The Role Artificial Intelligence in Modern Banking An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance.

networkreadinessindex. (2023). Retrieved from networkreadinessindex: networkreadinessindex.org

Venkata Siva Prakash Nimmagadda. (2021). Artificial Intelligence for Compliance and Regulatory Reporting in Banking: Advanced Techniques, Models, and Real-World Applications. *Journal of Bioinformatics and Artificial Intelligence*.

الفائز بالمركز الثاني

دراسة بحثية مشتركة للأستاذ/ حسين عبد الحميد حسين

والأستاذ/ حسن مجدي الشوربجي

المصرف المتحد

Artificial Intelligence Implementation for Cyber Security in Banking Industry.

Glossary:

- AI - Technology that enables systems to perform tasks requiring human intelligence.
- GDPR - European Union data protection law ensuring privacy and security of personal data.
- ML (Machine Learning) - A subset of AI for data-driven performance improvement.
- NLP (Natural Language Processing) - AI that helps computers understand human language.
- Anomaly Detection - Identifies unusual data patterns for threat detection.
- Predictive Analytics - Uses past data to forecast future cybersecurity threats.
- Phishing - Cyber-attack tricking users into revealing sensitive data.
- Ransomware - Malicious software that locks data until a ransom is paid.
- Malware - Software designed to damage or infiltrate systems.
- SOAR - Security Orchestration, Automation and Response.
- SIEM - Security information and event management used to Analyzes security alerts in real-time.
- Deep Learning - Advanced ML using multi-layered neural networks.
- Quantum Computing - New computing model impacting cybersecurity.
- Compliance - Meeting legal and policy standards in data security.
- Playbooks - Automated response workflows for security incidents.
- Threat Intelligence - Information on threats to guide security actions.
- Incident Response - Actions to manage and mitigate cybersecurity incidents.

Research Methodology: -

1. Research Design: -

A mixed-methods approach will jointly use qualitative and quantitative research to analyze the implementation of AI in banking cybersecurity.

2. Research Objectives: -

- Evaluate the status of the currently existing AI technologies applied within banking cybersecurity.
- Ascertain the effectiveness of AI-driven solutions in mitigating risks associated with cybersecurity.
- Identify various challenges and best practices for AI integration.

3. Literature Review:

- Analysis of past research into AI in cybersecurity.
- The assessment of the vulnerabilities in the banking sector.
- Determining the gaps in the literature regarding AI implementations.

4. Data Collection: -

The structured questionnaires will be forwarded to IT security professionals in general, focusing on AI use, effectiveness, resource allocation, and other critical issues. Qualitative: Semi-structured interviews will be conducted with CISOs, IT security analysts, AI vendors, and members of a regulatory body, while facilitating focus groups discussing challenges and success stories.

5. Sampling Strategy:

Target IT security professionals across banks, using a sample size of 100 survey responses and 10-15 interview participants to ensure diverse insights.

6. Data Analysis: -

A. Quantitative: The use of SPSS or R will be used for the purpose of statistical analysis.

B. Qualitative: The thematic analysis will categorize the insights on challenges and best practices.

7. Ethical Considerations

Participant confidentiality is guaranteed, with informed consent adhering to the provisions of GDPR.

8. Delimitations

The limited access to a variety of subjects may affect generalizability. Responses may contain personal perception, which may be different from industry realities.

9. Expected Outcomes

The study hopes to offer an insight into AI's role in banking cybersecurity, point towards some best practices, and give concrete steps for the implementation of AI.

Introduction:

The rapid development of digital banking has revolutionized services in the financial world completely by enabling users to access services for convenience and from virtually anywhere, anytime. This transformation has reshaped customers' expectations about the speed, access, and efficiency of financial services. In as much as digital banking increases access, it has also created an avenue for a myriad of cybersecurity threats that are becoming increasingly prevalent and complex.

The International Monetary Fund estimates that the 2022 Cybersecurity Artificial Intelligence Implementation for Cyber Security in Banking Industry Report recorded the cost of cybercrime to reach an estimated USD 1 trillion annually. Due to their nature, financial institutions such as banks are targeted a lot because of the amount of sensitive financial and personal information contained within them, more so than any other sector.

This ominously challenging atmosphere saw the emergence of AI as a pivotal partner for banks in their combat against cyber threats. By merging AI into cybersecurity, AI has armed banks with unequaled competence in identifying threats, acting faster, and carrying out predictive analytics, enabling them to be at the forefront of this race in terms of cybersecurity rather than just being victims. For instance, AI-driven systems can analyze a lot of transactional data in real time to find anomalies and suspicious patterns that suggest fraud, phishing attempts, or network intrusions. Through various forms of machine learning and natural language processing, AI further refines the picking up of newly developed threat vectors, making the technology dynamic and ever-changing, like the cybercriminal methods themselves.

With AI in cybersecurity, while significantly helping in many ways, also comes challenges like costly implementation, specialist talent requirements, and ethical issues around data privacy. The more these AI solutions are adopted, the more cybercriminals begin to find ways to outsmart them-or exploit them-further raising the stakes for banks in these ongoing cybersecurity battles.

This paper explores the adoption of AI in cybersecurity within the banking industry: its effectiveness, challenges of deployment, and potential future impact. This study will look to help define how AI can help boost the resilience of digital banking infrastructures while attempting to light the way on striking that critical balance between the leveraging of advanced technologies and securing customer trust in a digital-first world.

Figure 1:- Cyber Security Main concerns

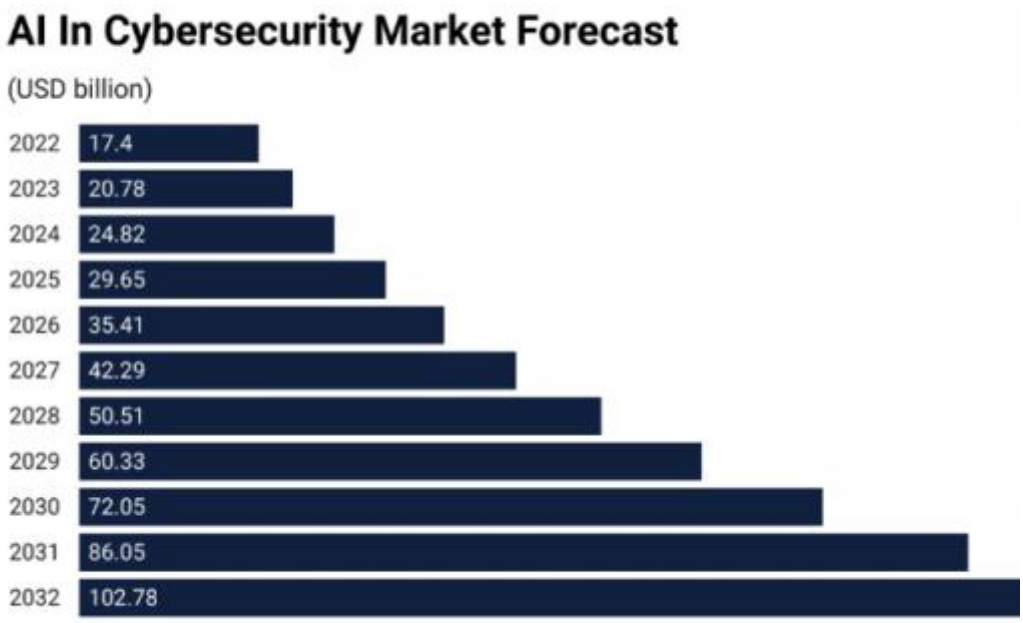


Figure 2: - AI Cyber Security Future Forecast

- Machine Learning Algorithms:

Here, large volumes of data are scanned by the ML algorithms for patterns that could intimate a cyber threat. Banks might use a subset called supervised learning, where the models are trained using historical attack data. This way, if similar patterns occur, they may be identified by the systems in real time.

Example: JPMorgan Chase uses machine learning algorithms in order to develop fraud detection systems. By analyzing transaction data, the bank can flag those that are out of the ordinary and may indicate fraud. - ----

- Natural Language Processing (NLP):

NLP as with any other organization, communication through channels should not be an easy task for phishing and other social engineering attacks. It analyzes the contents of emails and messages to identify suspicious sentences and phrases.

For instance, Bank of America uses NLP to monitor customers for traces of fraud and therefore often acts in quick time whenever the threat appears

imminent. It follows that many banks try to make the most of this facility and strive hard towards implementing technologies like fraud analytics.

- Anomaly Detection:

In anomaly detection, the approach is toward finding the deviation in normal behavior. This technique becomes important when it comes to real-time monitoring of transactions. AI-based systems flag those transactions that show deviation from set patterns.

Example: Citibank's fraud detection system applies anomaly detection in monitoring various transactions across accounts. This helps Citibank in shrinking the time taken for the identification and mitigation of fraud that may occur over time.

Predictive Analytics:

Predictive analytics apply past data to predict future cyber threats. Such a proactive approach prepares banks with an approach regarding potential attacks before they happen (Bourne, 2018).

Example: Wells Fargo uses predictive analytics when identifying trends and behaviors leading to an attack and determines the place where the security breach is.

Case Studies:

• HSBC: It implemented an AI-driven cybersecurity framework that reviews over 1.5 billion transactions per day, increasing its fraud detection rate by an extremely high amount. (HSBC, 2022).

Analysis of the Most Prevalent Cyber Attacks Against Banks Types of Cyber Threats:

• Phishing: This refers to when cyber attackers deceive users into revealing very important information. In 2021, the FBI reported that phishing was responsible for over $54 million in losses within the financial sector of the economy.

• Ransomware: Ransomware attacks encrypt bank data and demand a price for decryption.

The 2021 incident of the Colonial Pipeline showed that vulnerabilities exist in basic structures; banks fall under this category.

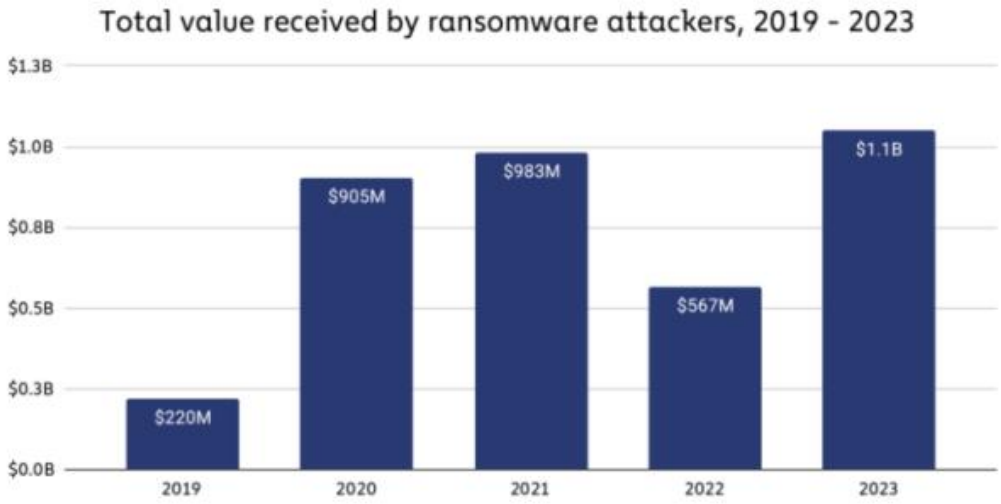


Figure 3: - Ransomware attacks financial impact.

• Malware: Malicious software created to penetrate systems; malware strikes on banks can translate to data breaches of really critical proportions. In the 2016 Bangladesh Bank heist, malware was used in the exploitation of banking systems (Krebs, 2016).

• Insider Threats: Employees can pose enormous insider threats through malicious intent or negligence. According to a report by the Ponemon Institute, insider threats account for 30% of all data breaches (Ponemon Institute, 2020).

Impact of Cyber Attacks on Banks:

The financial impact of a cyber-attack on banks could be catastrophic, including direct financial loss, regulatory fines, and reputational damage. One estimate puts the annual cost of cybercrime to the banking industry at $27.4 billion (Accenture, 2020).

Preventive Measures Using AI:

AI enhances prevention through:

- Constant monitoring of transactions and user behaviors.
- Automatic flagging of suspicious activities upon immediate investigation.
- Ability for immediate incident response to limit damages.

Figure 4: - Challenges in AI into Cybersecurity.

Data Privacy Concerns:

AI implementation involves substantial data-privacy and regulatory issues, including GDPR. The banks need to draw a proper line between the utility and privacy of the data. (Tikkinen-Piri et al., 2018).

Lack of Skilled Personnel Barriers to Effective Implementation of AI:

The shortage of skilled cybersecurity experts prevents effective implementation of AI. The workforce e in cybersecurity has to grow 65% to actively defend organizations against attacks according to (ISC)²,(ISC)², 2021).

- Integration with Legacy Systems: Most banks have been operating on legacy systems not tailored for modern AI integration. In most instances, this creates some inefficiencies and increased vulnerability as reported by multiple outlets.

- High Costs of AI Implementation: The first and foremost problem is that the initial investment in AI technologies can be unaffordable for the small banks. In general, according to Deloitte's report, the global total cost of cybersecurity is projected to surpass $1 trillion by 2025 (Deloitte, 2020).

- Ethical Issues: Being random in their nature, some AI processes sometimes create an appearance of biased results which may lead to the discriminative attitudes towards the clients. Banks have to be extra sensitive to these issues with the development of transparent and nondiscriminatory artificial intelligence use (Obermeyer et al., 2019).

Future of AI Technologies in Banking Cybersecurity Trends in AI Development:

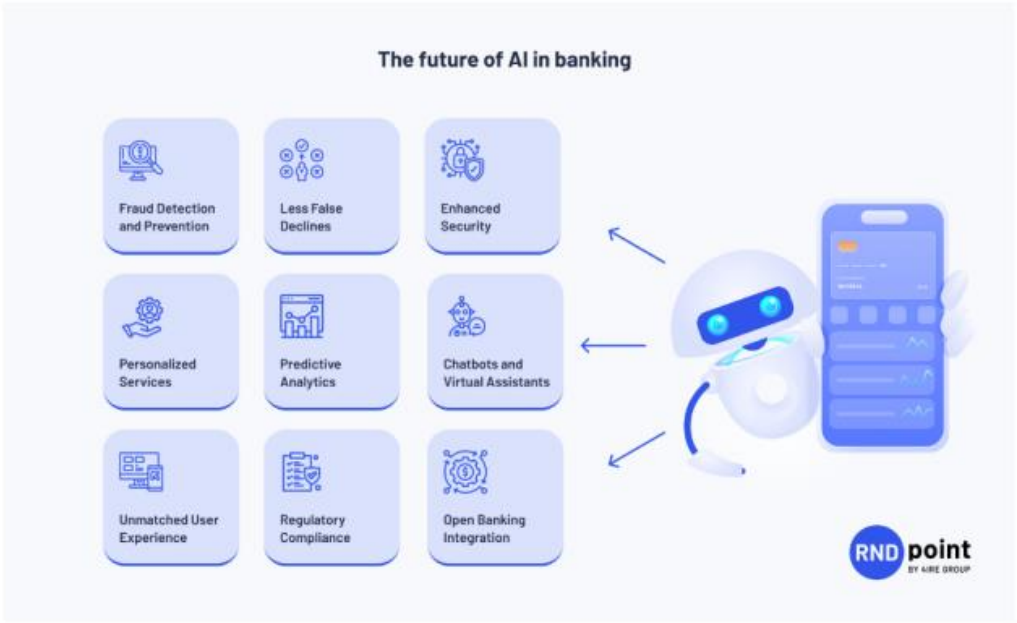


Figure 5: - Future of AI Technologies in Banking Cybersecurity.

The future of AI in banking cybersecurity is huge, wherein improvements in deep learning, federated learning, and quantum computing are expected to improve threat detection capabilities. The same has been indicated by the studies conducted by NIST (2021). Potential Advances in Threat Detection Next-generation AI technologies will enrich real-time threat analysis and response and thus enable banks to act against identified vulnerabilities before those vulnerabilities could be utilized for malicious activities. This is a view shared by IBM (2022).

- Role of AI in Regulatory Compliance:

AI can perform all those processes that are directly or indirectly related to compliance for the banks so that they remain within those complex regulations and at the same time ensure the risks associated with such processes are considerably reduced. Machine learning algorithms may observe transactions for compliance issues round the clock. (Finextra, 2021)

- Use Cases of AI Implementation:

• Barclays: AI-powered analytics developed for enhancing fraud detection and improvement in customer service through chatbots enabled by AI. (Barclays, 2022)

• Goldman Sachs: AI solutions have been implemented for risk management and compliance, making overall operations smoother and safeguarding data. AI in cybersecurity offers a range of benefits to the banking sector, from the level of detection up to threat prevention. Data privacy, shortage of skilled personnel, and integration are some of the concerns that need to be considered for actual deployment. As new technologies in AI are developed, the role it plays in protecting banking systems will be of greater importance.

Figure 6: - SOAR Operation Graph.

Adding on of AI program in cybersecurity, SOAR, it aims at enhancing the efficiency and effectiveness of security operations by putting together a suite

of security tools and processes into a combined workflow. They automate repetitive tasks, streamline incident response, and facilitate better collaboration among security teams.

Key Capabilities of SOAR Solutions:

- Integration: Security Orchestration, Automation, and Response solutions integrate with a wide range of security technologies, including SIEM, threat intelligence platforms, and endpoint detection solutions. In this way, SOAR becomes a general platform for responding to security-related incidents.

- Automation: With SOAR solutions, much of the manual work is automated in regular tasks such as triaging alerts, classifying incidents, and generating reports. This frees the valuable skills of security analysts to focus their attention on more complex investigations.

- Playbooks: The SOAR solution uses pre-programmed workflows or "playbooks," which are detailed, step-by-step processes applied to different security incident response scenarios. Such playbooks can be customized for exact organizational needs and threat landscapes.

- Collaboration: With SOAR, there will be increased collaboration among teams with shared visibility into incidents and a single platform through which communications and actions can be taken.

AI Use in the SOAR Solutions:

The use of AI in enhancing SOAR solutions has been observed along several dimensions:

- Threat Detection: AI algorithms sift through large volumes of data looking for patterns and anomalies that might indicate the presence of a potential threat. Over time, machine learning models self-learn and enhance their capability to be more efficient in detecting sophisticated attacks.
- Incident Prioritization: AI can assist in incident prioritization based on the extent of the damage and potential impact so that security teams

address the most critical incidents first. - Contextual Analysis: AI can provide context to any incident by correlating data from various sources, like user behavior analytics, historic data, and threat intelligence feeds. This gives the security analyst a better understanding of the situation.

- Automated Responses: AI can automatically perform certain responses, such as isolating the system that has become a victim of an attack or blocking malicious IP addresses, which speeds up the response times.
- Continuous Learning: AI learns from previous incidents and responses to continuously improve playbooks and future investigations.

Conclusion:

The implementation of AI in cybersecurity will have several benefits, therefore providing the banking sector with huge benefits regarding threat detection and prevention. Nonetheless, data privacy concerns, unavailability of skilled people, and integration are some of the challenges that must be overcome to successfully implement AI technologies.

Undeniably, the increasingly evolving nature of AI technologies will make them even more significant for the protection of banking systems in the near future.

Recommendations:

• Adopt machine learning for real-time threat detection: Deploy machine learning algorithms to analyze large volumes of data to spot patterns that are not normal and may be critical in identifying potential threats in real time. Anomaly detection does, for instance, spot deviations in user behavior, which reduces the time it takes to respond to threats.

• Natural Language Processing for Social Engineering Attack Prevention: NLP can parse email and other communications content for phishing and social engineering attempts. The layer of AI-driven analytics detects suspicious phrases and gives early warnings against potential attacks.

• Smarter Efficiency: Use Security Orchestration, Automation, and Response. AI-powered SOAR solutions can automate repetitive tasks, incident

classification, and reporting activities to free the security analysts for more complex investigations, hence improving overall efficiency.

• Key Challenges Addressed: AI and cybersecurity development are at a shortage. One should develop or train the already existing personnel for AI technologies and hire skilled professionals for the successful implementation and management of these systems.

• Ensure Compliance and Data Privacy: while AI may automate compliance checks, data privacy needs to be critically considered. Therefore, a framework should be developed that harmoniously balances the utility of AI with strict adherence to privacy regulation in such a way that the customer's data will be handled responsibly and securely.

References for authenticity of information check:

• Accenture. 2020. The Cost of Cybercrime: A 2020 Study of the Financial Services Sector.

• Barclays. (2022). Innovating Security with Artificial Intelligence.

• Bourne, M. (2018). Predictive Analytics in Cybersecurity: A Future Perspective. The Cybersecurity Journal.

• Canola, V., Banerjee, A., & Kumar, V. (2009). "Anomaly Detection: A Survey." ACM Computing Surveys, 41(3), 1-58.

• Deloitte. (2020). Cybersecurity Predictions 2021: New Trends in Risk Management.

• FBI. (2021). Internet Crime Complaint Center (IC3) Report

• Finestra. (2021). AI in Compliance: The Future of Regulatory Adherence in Banking.

• Goldman Sachs. (2022). Artificial Intelligence in Risk Management. Gonzalez, C., et al. 2021. "Challenges in Integrating AI in Banking Security." Journal of Financial Technology. HSBC. 2022. AI-Driven Cybersecurity Framework. ISC². 2021. Cybersecurity Workforce Study. IBM. 2022. The Future of AI in Cybersecurity. Khan, M., et al. 2020. "Machine Learning for Cybersecurity: Techniques and Applications." Journal of Cybersecurity. Kaspersky. 2020. DDoS Attacks on Financial Institutions: A 2020 Analysis. Krebs, B. 2016. "Inside the Bangladesh Bank Heist." Krebs on Security.

• NIST. 2021. AI and Cybersecurity: Future Trends.

• Obermeyer, Z. et al. 2019. "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations." Science, 366(6464): 447-453.

• Poleman Institute. 2020. 2020 Cost of Insider Threats Report.

• Ransomware Task Force. 2021. Combating Ransomware: A Comprehensive Framework.

• Tikkinen-Piri, C. et al. 2018. "EU General Data Protection Regulation: Changes and Implications for the Business." Computer Law & Security Review.

• Yin, J. et al., 2021. Natural Language Processing for Cybersecurity: A Review. ACM Computing Surveys.

الفائز بالمركز الثالث

الأستاذ/ أحمد رجب عبد العظيم

بنك التعمير والإسكان

استخدام الذكاء الاصطناعي في تعزيز الأمن السيبراني في البنو

المستخلص

يهدف هذا البحث إلى تقديم فهم واضح وبسيط للذكاء الاصطناعي، وتسليط الضوء على إمكانيات استخدامه في تعزيز الأمن السيبراني في البنوك، والفوائد التي يمكن أن تنعكس على الاقتصاد ككل من خلال التنفيذ الواسع النطاق، بالإضافة إلى التحديات التي قد تواجه هذا التطبيق والحلول المقترحة لتفادي تلك التحديات. تركز الدراسة على عرض الأبحاث السابقة وتحليل الدراسات المتعلقة باستخدام الذكاء الاصطناعي في تعزيز الأمن السيبراني. تم جمع البيانات والمعلومات المقدمة من التقارير والكتب والمقالات والأبحاث المنشورة حول الموضوع.

وخلصت الدراسة إلى أن استخدام الذكاء الاصطناعي في تعزيز الأمن السيبراني يساهم بشكل كبير في التنبؤ بالتهديدات المحتملة وضمان الاستجابة السريعة، فضلاً عن تقليل الوقت والتكاليف المرتبطة باكتشاف هذه التهديدات. والأثر الكبير للتقدم التكنولوجي لتأمين القطاع المصرفي ضد التهديدات المحتملة وتعزيز الأمن السيبراني. كما حددت الدراسة طرق منع التهديدات المحتملة وأكدت على ضرورة الاستثمار في الذكاء الاصطناعي وتدريب الموظفين وإعادة تقييم القوانين التي تحكم استخدام الذكاء الاصطناعي، حيث يجب تطوير هذه القوانين للتغلب على العقبات والتحديات التي تحول دون الاستفادة الفعالة من تقنيات الذكاء الاصطناعي مع ضمان أمن وسلامة البيانات.

كما حددت الدراسة الحاجة الملحة لإعادة الاستثمار في البنية التحتية للبنوك والمؤسسات لضمان أن يتماشى تشغيل تقنيات الذكاء الاصطناعي بشكل مثالي مع الأنظمة الداخلية لهذه المؤسسات، مما يعود بالنفع في نهاية المطاف على المؤسسة ويعزز أمنها السيبراني.

Abstract

This research aims to provide a clear and simple understanding of artificial intelligence, highlighting its potential use in enhancing cybersecurity in banks, the benefits it can bring to the economy as a whole through widespread implementation, and the challenges it faces along with possible solutions. The study focuses on presenting previous research and analyzing studies related to the use of artificial intelligence in bolstering cybersecurity. The data and information presented were gathered from reports, books, articles, and published research on the topic .

The study concluded that utilizing artificial intelligence in enhancing cybersecurity significantly contributes to predicting potential threats and ensuring rapid responses, as well as reducing the time and costs associated with threat detection. This has a major impact on advancing technology to secure the banking sector against potential threats and strengthen cybersecurity. The study also outlined ways to prevent potential threats and emphasized the necessity of investing in artificial intelligence, training personnel, and re-evaluating the laws governing the use of artificial intelligence. These laws should be developed to overcome the obstacles and challenges to effectively leveraging AI technologies while ensuring the security and safety of data.

Additionally, the study identified the urgent need to reinvest in the infrastructure of banks and institutions to ensure that the operation of artificial intelligence technologies aligns perfectly with the internal systems of these organizations, ultimately benefiting the institution and enhancing its cybersecurity.

مقدمة

أصبح الاعتماد على تقنيات الذكاء الاصطناعي في مختلف المؤسسات وجوانب الحياة أمرًا ضروريًا لا غنى عنه. يُعتبر استخدام الذكاء الاصطناعي في تعزيز الأمن السيبراني في البنوك أحد أهم التطبيقات، حيث يُعد الأمن السيبراني قضية حيوية تواجه البنوك مع تزايد التهديدات السيبرانية حيث تواجه المؤسسات عددًا متزايدًا من الهجمات المتطورة مما يدفعها للبحث عن طرق جديدة لحماية معلوماتها وأنظمتها الحساسة. لذلك، أصبحت الحاجة ملحة لتبني تقنيات حديثة مثل الذكاء الاصطناعي لتعزيز الحماية والوقاية من الهجمات.

يستعرض هذا البحث كيفية استخدام الذكاء الاصطناعي في تعزيز الأمن السيبراني للبنوك، مع التركيز على الأساليب والتقنيات المتاحة وكيفية تحقيق أقصى استفادة منها في مواجهة التهديدات الحالية والمستقبلية. حيث يمكن من خلال الذكاء الاصطناعي أتمتة عمليات الأمن السيبراني وتحديد التهديدات والاستجابة لها في الوقت الفعلي.

يساهم الذكاء الاصطناعي في تقديم تقارير دقيقة حول نقاط الضعف وكيفية معالجتها، مما يعزز من فعالية استراتيجيات التأمين. كما يمكن أن يُبسط إجراءات التدقيق الداخلي، مما يؤدي إلى تحسين الدقة وزيادة الرؤية في العمليات داخل المنظمة. يمكن للذكاء الاصطناعي، من خلال تحليل كميات هائلة من البيانات، الكشف عن الأنماط غير العادية والتنبؤ بالتهديدات المحتملة، مما يعزز من قدرة البنوك على حماية معلوماتها وأنظمتها الحساسة وبالتالي يعتبر الذكاء الاصطناعي عنصرًا محوريًا في تطوير آليات الأمن السيبراني، مما يتيح للبنوك البقاء على أهبة الاستعداد لمواجهة التحديات المتزايدة في هذا المجال.. (Dambe et al., 2023)

أدى التطور التكنولوجي وزيادة الوعي العام بأهمية الأمن السيبراني، إلى جانب تنفيذ اللوائح وإنفاذ القانون، وحجم البيانات المتاحة من مصادر متعددة، إلى جعل استخدام حلول موثوقة ومُعززة للأمن السيبراني أمرًا ضروريًا في جميع الصناعات. ويرجع سبب تطور أنظمة الأمن السيبراني المعتمدة على تقنيات الذكاء الاصطناعي إلى ارتفاع وتيرة ومستوى الهجمات السيبرانية حيث أدى التطور الهائل في التكنولوجيا إلى زيادة التهديدات والهجمات الإلكترونية، مما دفع جميع المؤسسات إلى ضرورة إيجاد حلول فعّالة لتأمين بياناتها. تتعاون المجموعات الإجرامية فيما بينها، حيث تتبنى خططًا متطرفة لسرقة المعلومات عبر الحدود الدولية، وتتنافس لتحقيق مكاسب مالية على حساب الآخرين.

وبناءً عليه، فإن الهدف الأساسي من معظم الهجمات الإلكترونية هو الربح، مما يبرز الحاجة الملحة لتعزيز استراتيجيات الأمن السيبراني والتكيف مع التهديدات المتزايدة. (Tao et al., 2021)

المسألة البحثية

أدى التطور السريع في التكنولوجيا وزيادة استخدامها في جميع المجالات إلى ارتفاع احتمالات وجود تهديدات وهجمات سيبرانية مُحكمة التخطيط وقد نتج عن ذلك ضرورة استخدام الذكاء الاصطناعي لتعزيز مواجهة هذه الهجمات من خلال تحسين الأمن السيبراني وتعزيز آليات العمل في الأنظمة المختلفة.

وبناء عليه فان السؤال الرئيسي للبحث هو

كيف يتم استخدام تقنيات الذكاء الاصطناعي للكشف عن التهديدات السيبرانية ومنعها؟

أهداف البحث

1- التعرف على الهجمات السيبرانية وأنواعها
2- تحليل أنواع الهجمات السيبرانية الشائعة التي تستهدف البنوك وكيفية الوقاية منها.
3- توضيح التحديات التي تواجه استخدام الذكاء الاصطناعي في الامن السيبراني .
4- ما هو المتوقع لتقنيات الذكاء الاصطناعي في حماية الا نظمة المصرفية

مصطلحات تم استخدامها في البحث

الذكاء الاصطناعي: الذكاء الاصطناعي هو تطوير أجهزة الكمبيوتر التي تستطيع القيام بالمهام البشرية مثل التعرف على الكلام وإمكانية الادراك البصري. واتخاذ القرارات بدقه في حالة عدم التأكد - مستوحى من (Tom, et al, 2018, p.3) - يمكن تعريفه أيضا على انه مزيج من الأتمتة المعرفية، التعليم الألى وامكانية البحث والاستدلال، معالجه البيانات مما يمكن من اخذ القرارات والقيام بالمهام البشرية والتفوق عليها - مستوحى من (Villar & Khan , 2021. P 74)

الأمن السيبراني: هو مجال يركز على حماية الأنظمة الحاسوبية والشبكات والمعلومات الرقمية من التهديدات والهجمات الإلكترونية. يهدف هذا المجال إلى تأمين البيانات ومنع وكشف والاستجابة لانتهاكات الأمن والهجمات التي تستهدف الأفراد والمؤسسات. يتضمن الأمن السيبراني تحليل المخاطر

وتصميم وتنفيذ إجراءات أمان ضرورية لحماية البيانات والشبكات، بالإضافة إلى التعامل الفعال مع حوادث الأمن يُعتبر الأمن السيبراني عنصرًا أساسيًا للحفاظ على سرية المعلومات وضمان استمرارية العمليات الحاسوبية والاتصالات المرتبطة بها (المصري، 2024).

منهجية البحث:

في هذا البحث، تم اعتماد المنهج الوصفي التحليلي لدراسة ومراجعة بعض الدراسات والأبحاث السابقة المتعلقة بدور الذكاء الاصطناعي في تعزيز الأمن السيبراني. يهدف هذا المنهج إلى استخلاص النتائج التي تم ذكرها في البحث، مع التركيز على توضيح كيفية تأثير الذكاء الاصطناعي في هذا المجال، بالإضافة إلى التعرض للتحديات التي تواجه استخدامه ومحاولة إيجاد الحلول المناسبة لها

فهم الذكاء الاصطناعي – تعريفه وانواعه

بدأ الذكاء الاصطناعي في الظهور في منتصف القرن العشرين وكان اختراع البحرية الامريكية للكمبيوتر في عام 1938 وظهور الكمبيوتر الرقمي بعدها سنه 1939 بواسطة **Konardzuse** من أهم العوامل التي ساهمت في اختراع الذكاء الاصطناعي.

وفى عام 1956 وتحديدا في كليه دارتموث قام كل من **Marvin Minsky**و **John McCarthy** بتنظيم ورشة عمل حيث تم استخدام اول مصطلح للذكاء الاصطناعي بها [0]

بات مصطلح ال **Artificial Intelligence** شائعا ويتردد كثيرا في الآونة الأخيرة في المجالات التقنية حيث تكمن قدره الذكاء الاصطناعي في محاكاة الذكاء البشرى ولكن يتفوق عليه بشكل هائل في السرعة والكم وتنفيذ المهام المختلفة بدقه تم اعدادها واختبارها مسبقا.

أنواع الذكاء الاصطناعي:

1. **الذكاء الاصطناعي البسيط :**وهو ذلك النوع البسيط الموجود بالهواتف الذكية وأجهزة الكمبيوتر والأجهزة المنزلية التقليدية ويعرف باسم (Embedded AI)

2. **الذكاء الاصطناعي المتطور:** وهو نوع اكثر تطورا حيث يمكن له التعلم مع مرور الوقت بحيث يمكنه القيام ببعض المهام التي يقوم بها العقل البشرى وتعرف باسم (Developmental AI)
3. **الذكاء الاصطناعي الفائق**: وهو ذلك النوع الذي يمكن له محاكه العقل البشرى بل ويتفوق عليه أيضا من حيث الوعي والفهم وإيجاد الحلول ويعرف باسم **:**(Conscious AI)

ولكن يعد الذكاء الاصطناعي الفائق مفهوما افتراضيا ليس له وجود حقيقي حتى الان

كيفية استخدام تقنيات الذكاء الاصطناعي للكشف عن التهديدات السيبرانية ومنعها.

تقنيات الذكاء الاصطناعي (AI) تلعب دورًا متزايد الأهمية في مجال الأمن السيبراني حيث يوجد العديد من الطرق التي يمكن بها كشف التهديدات السيبرانية باستخدام الذكاء الاصطناعي

"Cybersecurity and Artificial Intelligence: A Comprehensive Guide" (2022)

1- تحليل البيانات الضخمة:

يمكن للذكاء الاصطناعي تحليل كميات هائلة من البيانات واكتشاف الأنماط غير المعتادة التي قد تشير إلى هجوم عن طريق استخدم خوارزميات التعلم الآلي التي يمكن من خلالها فهم وتحليل أي عدد من البيانات والربط بينهم في وقت قصير جدا والوصول الى أفضل النتائج والتوصيات.

2- الكشف عن التسلل:

يمكن للذكاء الاصطناعي أن يكتشف حالات التسلل والاختراق من خلال التعرف على الأنشطة غير الطبيعية في الشبكة. يقوم بذلك عن طريق مراقبة حركة المرور، حيث يستطيع التعرف على اي سلوكيات غير نمطية، مما يساعد في اكتشاف محاولات التسلل في الوقت المناسب.

3- التصنيف التلقائي:

- عن طريق جمع البيانات والمعلومات وتصنيفها يمكن ان يتم استخدام ال AI لتحديد أنواع التهديدات (مثل البرمجيات الخبيثة، والفيروسات، وغيرها) بناءً على سلوكها.

4- استجابة تلقائية:

- يمكن للأنظمة الذكية التي يستخدمها الذكاء الاصطناعي في اتخاذ إجراءات استباقية تلقائية عند اكتشاف تهديد محتمل او استشعار حركه غير نمطيه او محاولات مرور مستمرة بشكل غير امن الى اتخاذ اجراء وقائي مثل حظر عنوان IP المشتبه فيه أو عزل الأجهزة المتأثرة.

5- تحليل سلوك المستخدمين:

يعتبر تحليل سلوك المستخدمين باستخدام الذكاء الاصطناعي أداة فعّالة لكشف التهديدات السيبرانية. يعتمد هذا النوع من التحليل على جمع البيانات السلوكية وتحليلها لتحديد الأنماط الشاذة. على سبيل المثال، إذا كان مستخدم معين يسجل الدخول عادةً من موقع محدد ثم سجل الدخول من موقع غير مألوف في وقت غير اعتيادي، فقد يشير ذلك إلى وجود تهديد محتمل.

6- تحسين الأنظمة:

- يمكن للذكاء الاصطناعي المساهمة في تحسن الأنظمة المستخدمة في البنوك عن طريق استخدام التعلم العميق والمستمر من الهجمات المختلفة السابقة وتحليل حركات المرور على الشبكة وتحديد الأنشطة غير المعتادة حيث يمكن من خلال ذلك تحسين قدرة الأنظمة على التعرف على التهديدات الجديدة والمتطورة.

7- التنبؤ بالتهديدات المستقبلية:

تساعد خوارزميات التعلم الآلي التي يعتمد عليها الذكاء الاصطناعي في التنبؤ بالتهديدات المستقبلية المحتملة من خلال تحليل البيانات التاريخية المجمعة، مثل سجلات المعاملات والتفاعلات عبر الإنترنت. يقوم بتحليل سلوك المستخدمين والنظام بشكل مستمر، مثل محاولات الدخول المتكررة أو التحويلات المالية المشبوهة. كما يمكن للذكاء الاصطناعي تحديد نقاط الضعف في البنية التحتية الأمنية للبنك وتقديم توصيات لتعزيز الأمان.

- يمكن استخدام AI للكشف عن رسائل البريد الإلكتروني الاحتيالية من خلال تحليل محتوى الرسائل وسلوك المرسل وتحليل السمات مثل - العنوان (Subject) وكلمات مفتاحية محددة - المرسل (Sender)وعنوان البريد الإلكتروني – تحليل نص الرسالة نفسه وتحليل اللغة المستخدمة - الروابط الموجودة داخل الرسالة حيث يتم استخدام النموذج المدرب لمراقبة البريد الوارد في الوقت الحقيقي وتنبيه المستخدمين عن الرسائل المشتبه فيها.

9- التحديث المستمر:

- يعتمد الذكاء الاصطناعي على التحديث المستمر للأنظمة المستخدمة حيث تتعلم الأنظمة من التجارب السابقة ومن تحليلها المستمر للبيانات وتتحسن مع الوقت وتزداد فاعليتها وقوتها في مواجهة التهديدات الجديدة. من خلال هذه التقنيات التي تم شرحها، يمكن للبنوك والمؤسسات تعزيز دفاعاتها السيبرانية وتحديث أنظمتها بشكل مستمر. يساعد ذلك في تحديد أوجه القصور ونقاط الضعف في الأنظمة الإلكترونية المختلفة، مما يقلل من مخاطر الهجمات الإلكترونية.

الهجمات السيبرانية

أولا: تعريف الهجمات السيبرانية :

هي محاولات غير مصرح بها للوصول إلى الأنظمة أو البيانات بهدف سرقتها أو تدميرها أو تعطيلها تشمل هذه الهجمات مجموعة متنوعة من الأنشطة الضارة، مثل الفيروسات، والبرامج الضارة، وهجمات حجب الخدمة(DDoS) ، والهندسة الاجتماعية.("Cybersecurity Essentials" - Cisco Networking Academy).

ثانيا: أنواع من الهجمات السيبرانية:

1- هجمات التصيد (Phishing): تهدف إلى خداع المستخدمين للكشف عن معلوماتهم الحساسة مثل كلمات المرور أو تفاصيل البطاقة الائتمانية من خلال رسائل إلكترونية مزيفة.

3- هجمات حجب الخدمة (DDoS): هي نوع من الهجمات السيبرانية تهدف إلى إعاقة عمل خادم أو شبكة أو خدمة عبر إغراقها بكمية هائلة من حركة البيانات غير المشروعة يتم تنفيذ هذه الهجمات من خلال استخدام العديد من الأجهزة المتصلة بالإنترنت (مثل الحواسيب المخترقة) التي تُعرف باسم "بوت نت".

4- الهجمات القائمة على الثغرات (Exploitation) : تستغل نقاط ضعف في البرمجيات أو الأنظمة للوصول غير المصرح به.

5- الهجمات الداخلية (Insider Threats): تتم من قبل موظفين أو أشخاص لديهم إمكانية الدخول بشكل مشروع على النظام ويستخدمونه بشكل غير مشروع.

6- الهجمات على الشبكات (Network Attacks) : تشمل التجسس على البيانات المتداولة عبر الشبكة أو محاولة اختراق الشبكات.

7- هجمات تكسير كلمات المرور (Password Cracking): تهدف إلى تخمين أو كسر كلمات المرور للوصول إلى حسابات المستخدمين.

-كتاب "Cybersecurity Essentials"

ثالثا : تحليل أنواع الهجمات السيبرانية الشائعة التي تستهدف البنوك وكيفية الوقاية منها

وفقًا لتقارير متعددة، شهدت مصر زيادة ملحوظة في الهجمات السيبرانية خلال السنوات الأخيرة. في عام 2021، أفادت التقارير بأن الهجمات السيبرانية استهدفت مؤسسات حكومية ومراكز بيانات وشركات خاصة. وفقًا لتقرير شركة "Check Point" للأمن السيبراني، فقد تصدرت مصر قائمة الدول الأكثر تعرضًا للهجمات السيبرانية في الشرق الأوسط - على سبيل المثال، في عام 2020، ذكرت شركة "Cisco" أن 60% من المؤسسات المصرية تعرضت لهجمات سيبرانية. بينما أشار تقرير "Threat Intelligence Report" الصادر عن "Kaspersky" إلى أن هناك زيادة بنسبة 45% في عدد الهجمات السيبرانية في مصر مقارنة بالسنوات السابقة مما يتطلب استراتيجيات فعالة للوقاية. ونستعرض فيما يلي تحليل لبعض أنواع الهجمات الشائعة وطرق الوقاية منها:

الهجمات بالبرمجيات الخبيثة (Malware): الهجمات بالبرمجيات الخبيثة (Malware) تشير إلى البرامج الضارة التي تُستخدم لاختراق الأنظمة وسرقة المعلومات أو تدمير البيانات.

الأنواع الشائعة من البرمجيات الخبيثة:

- الفيروسات: تتنقل عبر الملفات وتقوم بتكرار نفسها عند فتح الملف المصاب.

- البرمجيات التجسسية (Spyware): تُجمع المعلومات حول المستخدمين دون علمهم.

-برامج الفدية (Ransomware): تشفر الملفات وتطلب فدية لفك التشفير.

-التروجان (Trojan): تتظاهر بأنها برامج شرعية ولكنها تخفي وظائف ضارة.

كيفية الوقاية من الهجمات بالبرمجيات الخبيثة:

1- استخدام برامج مكافحة الفيروسات: تثبيت برنامج موثوق لمكافحة الفيروسات وتحديثه بانتظام مع تفعيل الجدران النارية لحماية الشبكة (Firewalls)

2- تحديث النظام والبرامج: التأكد من تحديث نظام التشغيل والبرامج بشكل دوري لسد الثغرات الأمنية مع حفظ نسخ احتياطية من البيانات المهمة في مكان آمن

3- التوعية والتدريب: تثقيف المستخدمين حول مخاطر البرمجيات الخبيثة وأساليب الاحتيال.

موقع"Cybersecurity & Infrastructure Security Agency (CISA)"

الهجمات بوسائل الهندسة الاجتماعية (Social Engineering)

الهجمات بوسائل الهندسة الاجتماعية هي أساليب يستخدمها المهاجمون لخداع الأفراد أو المنظمات لكسب معلومات حساسة، مثل كلمات المرور أو المعلومات المالية، من خلال التلاعب النفسي بدلاً من استغلال الثغرات التقنية.

أنواع الهجمات:

- التصيد الاحتيالي (Phishing): إرسال رسائل بريد إلكتروني مزيفة تبدو وكأنها من مصدر موثوق، تطلب من الضحية إدخال معلوماته الشخصية.
- التصيد الصوتي (Vishing): استخدام المكالمات الهاتفية للحصول على معلومات حساسة من الضحية.
- التصيد النصي (Smishing): إرسال رسائل نصية تحتوي على روابط أو طلبات معلومات.
- الهندسة الاجتماعية المباشرة: التظاهر بأن الشخص يتبع إجراءً رسميًا للحصول على المعلومات.
- هجمات "البيرستينغ" (Baiting): تقديم شيء جذاب (مثل ملف مجاني) لتحفيز الضحية على تحميل برمجيات ضارة.

كيفية الوقاية:

- التوعية والتدريب: تعليم الموظفين كيفية التعرف على محاولات الهندسة الاجتماعية.
- التحقق من الهوية : التأكد من هوية الأشخاص قبل تقديم أي معلومات حساسة.
- تجنب الروابط المشبوهة : عدم النقر على الروابط أو تحميل الملفات من مصادر غير موثوقة.
- استخدام التحقق الثنائي : تفعيل ميزة التحقق الثنائي لحماية الحسابات.
- تحديث البرامج : التأكد من تحديث البرامج ونظم التشغيل بشكل دوري لسد الثغرات الأمنية.

كتاب "Social Engineering: The Art of Human Hacking" لمؤلفه **Kevin Mitnick**. حول الهندسة الاجتماعية

الهجمات من نوع "DDoS" (Denial of Service)

الهجمات من نوع "DDoS" (Denial of Service) هي هجمات تهدف إلى إغراق خادم أو شبكة أو خدمة معينة بكمية هائلة من البيانات أو الطلبات مما يؤدي إلى تعطيل الخدمة أو جعلها غير متاحة للمستخدمين الشرعيين يُعتبر "DDoS" نسخة موزعة من الهجوم التقليدي حيث تُستخدم فيها مجموعة من الأجهزة المخترقة (مثل أجهزة الكمبيوتر أو الهواتف الذكية) للتحكم بها عن بعد.

أنواع هجمات DDoS:

- -هجمات الطبقة السابعة (Application Layer): تستهدف التطبيقات والخدمات على الشبكة.
- هجمات الطبقة الرابعة (Transport Layer): تستهدف بروتوكولات النقل مثل TCP وUDP.
- -هجمات الطبقة الثالثة (Network Layer): تستهدف البنية التحتية للشبكة، مثل الروترات والخوادم.

كيفية الوقاية منها:

- استخدام خدمات الحماية: مثل خدمات الحماية من DDoS التي تقدمها شركات متخصصة، مثل Cloudflare أو Akamai.
- زيادة السعة: تحسين البنية التحتية وزيادة السعة لتحمل ضغط أكبر من الطلبات.
- توزيع الحمل: استخدام تقنيات توزيع الحمل (Load Balancing) لتوجيه حركة المرور عبر عدة خوادم.
- التصفية: إعداد جدران نارية (Firewalls) وأنظمة كشف التسلل (IDS) لتصفية الحركة المشبوهة.
- استجابة سريعة: وضع خطة استجابة للطوارئ تتضمن إجراءات سريعة للتخفيف من تأثير الهجمات عند حدوثها.
- تحديث البرمجيات: الحفاظ على تحديث جميع الأنظمة والبرمجيات لتفادي الثغرات الأمنية التي قد يستغلها المهاجمون.

"CISA" (Cybersecurity & Infrastructure Security Agency) حول أمان الشبكات وطرق الحماية من هجمات DDoS

الهجمات على التطبيقات المصرفية (Web Application Attacks)

- الهجمات على التطبيقات المصرفية (Web Application Attacks) تشمل مجموعة من التقنيات التي يستغلها المهاجمون لاستهداف الأنظمة والتطبيقات المصرفية عبر الإنترنت. من أبرز هذه الهجمات:
- حقن SQL (SQL Injection) : استغلال ثغرات في قواعد البيانات من خلال إدخال أوامر SQL ضارة.
- التلاعب بالجلسات (Session Hijacking) الاستيلاء على جلسات المستخدمين الشرعيين للوصول إلى حساباتهم
- هجمات XSS (Cross-Site Scripting): إدخال نصوص برمجية ضارة في صفحات الويب التي يراها المستخدمون.

كيفية الوقاية

1- استخدام الاستعلامات المعدة مسبقًا (Prepared Statements) والتحقق من صحة المدخلات.
2- ا استخدام تشفير الجلسات يساهم التشفير في حماية البيانات المنقولة أثناء الجلسة، بينما يساعد إنهاء الجلسات غير النشطة على تقليل فرص الوصول غير المصرح به إلى المعلومات الحساسة
3- استخدام تشفير المحتوى (Content Encoding) وتحقق من المدخلات.
4- توعية المستخدمين، واستخدام بروتوكولات الأمان مثل HTTPS.
5- فرض قيود على عدد المحاولات، واستخدام التحقق الثنائي (Two-Factor Authentication).
6- إجراء اختبارات أمان دورية (Penetration Testing) لتحديد الثغرات

- OWASP (Open Web Application Security Project) -
- NIST (National Institute of Standards and Technology) –

الهجمات عبر الشبكات (Network Attacks)

الهجمات عبر الشبكات (Network Attacks) هي محاولات غير مصرح بها لاستغلال نقاط الضعف في الشبكات بهدف الوصول إلى المعلومات أو إتلافها أو تعطيلها. تتنوع هذه الهجمات بين عدة أنواع منها:

- التنصت (Sniffing): حيث يقوم المهاجم بالتقاط البيانات المتبادلة عبر الشبكة.

- الهجمات على الشبكة اللاسلكية (WLAN Attacks): مثل هجمات "Man-in-the-Middle" و"Rogue Access Points".

كيفية الوقاية من الهجمات:

1- استخدام جدران الحماية (Firewalls): لمنع الوصول غير المصرح به إلى الشبكة.
2- تشفير البيانات يساعد التشفير في تأمين البيانات ويعزز الخصوصية ويقلل من مخاطر الاختراق
3- تحديث الأنظمة بانتظام- يُعتبر ضرورياً لضمان تصحيح أي ثغرات معروفة. يساعد هذا التحديث في تعزيز الأمان ويقلل من فرص استغلال الثغرات من قبل المهاجمين.
4- استخدام بروتوكولات أمان قوية: مثل WPA3 في الشبكات اللاسلكية.
5- توعية الموظفين حول مخاطر الأمن السيبراني وكيفية التصدي للهجمات.

- Stallings, W. (2017). *Network Security Essentials: Applications and Standards*. 5th Edition. Pearson.

الهجمات الداخلية (Insider Threats)

تمثل تهديدات تنشأ من داخل المنظمة، حيث يكون الجاني موظفًا أو متعاقدًا أو أي شخص آخر لديه وصول إلى نظام المعلومات.

استراتيجيات الوقاية من الهجمات الداخلية:

1- تدريب الموظفين: توفير دورات تدريبية لرفع الوعي بأمن المعلومات وتعريفهم بالتهديدات الداخلية.
2- صلاحيات الوصول: تقليص حقوق الوصول إلى المعلومات الحساسة إلى الحد الأدنى المطلوب لأداء المهام.
3- مراقبة النشاطات: استخدام أدوات لمراقبة وتحليل الأنشطة ضمن الشبكة للكشف عن الأنماط غير المعتادة.
4- تطبيق سياسات صارمة: وضع سياسات واضحة للتعامل مع البيانات الحساسة وكيفية استخدامها بطريقة آمنة.
5- إجراء تقييمات منتظمة: - إجراء تقييمات دورية لتحديد الثغرات الأمنية وتحليل المخاطر.
6- تشجيع الإبلاغ عن الأنشطة المشبوهة: إنشاء نظام يسهل على الموظفين الإبلاغ عن أي سلوك غير اعتيادي أو مريب، مما يعزز ثقافة الأمان داخل المنظمة.

كتاب "Insider Threats in Cyber Security" للكاتب -Moor .H .J

التحديات التى تواجه استخدام الذكاء الاصطناعى فى الامن السيبرانى

على الرغم من الفوائد الكبيرة لدمج الذكاء الاصطناعي في الأمن السيبراني، إلا أنه يقدم أيضًا مجموعة من التحديات الخاصة. من المخاوف الرئيسية "إساءة استخدام الذكاء الاصطناعي من قبل الجهات الخبيثة"، حيث يمكن للقراصنة استغلال هذه التكنولوجيا لتطوير هجمات أكثر تعقيدًا واستهدافًا، وأتمتة مراحل مختلفة من عملياتهم. هذا قد يؤدي إلى سباق تسلح بين الهجمات والدفاعات المعتمدة على الذكاء الاصطناعي، مما يزيد من تعقيد مشهد الأمن السيبراني.

التحدي الآخر يتمثل في الآثار الأخلاقية لاستخدام الذكاء الاصطناعي في هذا المجال. كما أشار المستشار الأكاديمي في جامعة سان خوسيه الحكومية في كاليفورنيا، تثير الأنظمة المستقلة للذكاء الاصطناعي تساؤلات حول المساءلة. فمَن يكون المسؤول عندما يتخذ نظام أمني مدفوع بالذكاء الاصطناعي قرارًا يؤدي إلى عواقب غير مقصودة- إن تحقيق التوازن المناسب بين الاستقلالية والإشراف البشري يعد أمرًا بالغ الأهمية لتفادي النتائج السلبية غير المرغوب فيها.

علاوة على ذلك، يتطلب تكامل الذكاء الاصطناعي وجود قوة عاملة ماهرة قادرة على فهم تعقيدات كل من الأمن السيبراني وتقنيات الذكاء الاصطناعي. ونظرًا لنقص المهنيين ذوي الخبرة في كلا المجالين، يتضح الحاجة الملحة إلى التدريب والتعليم متعدد التخصصات. (مقاله عن - أبرز تحديات الأمن السيبراني مع تقدم الذكاء الاصطناعي؟ موقع skynewsarabia)

بالإضافة الى ان استخدام الذكاء الاصطناعي في الأمن السيبراني يواجه عدة تحديات منها:

1- جودة البيانات والثقافة السائدة

تعتمد قوة وقدرة الذكاء الاصطناعي على جودة البيانات المدرجة والتي يتم تحليلها وربطها بخوارزميات من شأنها الوصول الى نتائج سليمه. ففي بعض المؤسسات المالية جرى العرف على ترك عنصر بشرى لمراقبه العمليات المالية والتأكد من سلامتها. كما يمكن ان تكون ثقافة المؤسسة عائق امام التوسع في استخدام الذكاء الاصطناعي على نطاق واسع

2-الهجمات المتقدمة: يستفيد المهاجمون من الذكاء الاصطناعي لتطوير هجمات متطورة، مثل هجمات الشبكات العصبية، التي تستطيع تجاوز الدفاعات التقليدية.

3-**التحذيرات الكاذبة:** قد تؤدي نماذج الذكاء الاصطناعي إلى زيادة كبيرة في التحذيرات الكاذبة، مما يسبب إرباكًا للمختصين في الأمن ويؤثر سلبًا على فعالية استجاباتهم.

4-تكلفة التنفيذ: قد تكون تكلفة استثمار الموارد في تطوير وتنفيذ أنظمة ذكاء اصطناعي فعّالة مرتفعة، مما يمثل تحديًا للعديد من المؤسسات.

5- صعوبة التفسير: تعتبر بعض نماذج الذكاء الاصطناعي "صناديق سوداء" مما يجعل من الصعب تفسير كيفية اتخاذ القرارات، مما يؤثر على الثقة في الأنظمة.

6-**التكامل مع الأنظمة الحالية:** يمكن أن يكون دمج تقنيات الذكاء الاصطناعي مع أنظمة الأمان القائمة عملية معقدة، مما يستلزم موارد إضافية.

7- **تحديات التشريع والتنظيم:** القوانين المتعلقة بحماية البيانات واستخدام الذكاء الاصطناعي قد تحتاج إلى تعديلات لتواكب التطورات السريعة في هذا المجال.

حيث تتطلب هذه التحديات استراتيجيات مبتكرة لمواجهة المخاطر وتعزيز فعالية الأمن السيبراني.تقرير من "Gartner" بعنوان "AI in Cybersecurity: The Future of Threat Detection and Response" (2021).

المستقبل المتوقع لتقنيات الذكاء الاصطناعي في حماية الانظمة المصرفية

يتطور مجال الذكاء الاصطناعي بسرعة وتعقيد، مما يجعل غير الخبراء يعتقدون أنه من الصعب السيطرة عليه. بالإضافة إلى ذلك، قد يؤدي استخدامه إلى زيادة مخاطر المؤسسات الحالية أو تغيير طرق عرضها، أو حتى إدخال مخاطر جديدة. من المعروف أن صناعة الخدمات المالية هي مجال شديد التنظيم، يضم مجموعة كبيرة ومتداخلة من نماذج الأعمال والمنتجات، مما يتطلب من الشركات الالتزام بمستوى مناسب من الحذر في إدارة أعمالها حيث يمكن لتقنيات الذكاء الاصطناعي أن تُحدث تحولاً كبيرًا في كيفية حماية الأنظمة المصرفية، مما يعزز فعالية الإجراءات الأمنية ويقلل من المخاطر.

من خلال تحليل كميات هائلة من بيانات المعاملات، تستطيع نماذج الذكاء الاصطناعي تحديد الأنماط غير العادية التي قد تشير إلى أنشطة احتيالية. يمكّن هذا النهج الاستباقي البنوك من تقليل المخاطر بشكل أكثر فعالية وحماية أصول العملاء. ومع ذلك، يبقى الحفاظ على خصوصية البيانات والامتثال للمتطلبات التنظيمية أمرًا بالغ الأهمية لضمان ثقة العملاء وتلبية معايير الصناعة.

فيما يلي بعض الاتجاهات المتوقعة:

1-تحليل البيانات الكبيرة: يمكن للذكاء الاصطناعي معالجة كميات هائلة من البيانات في وقت قصير، مما يساعد في اكتشاف الأنماط السلوكية غير الطبيعية التي قد تشير إلى عمليات احتيال.

2.-الكشف عن الاحتيال في الوقت الحقيقي: استخدام تقنيات مثل التعلم الآلي لتحديد الأنشطة المشبوهة في الوقت الفعلي، مما يقلل من الخسائر المالية.

3-تعزيز الأمن السيبراني: يمكن للذكاء الاصطناعي أن يتنبأ بالتهديدات السيبرانية من خلال تحليل سلوك الشبكة، مما يساعد في اتخاذ إجراءات استباقية.

4-تحسين خدمة العملاء: الروبوتات الذكية والمساعدات الافتراضية يمكن أن تقدم دعماً سريعاً وفعالاً للعملاء مما يقلل من الضغط على الفرق البشرية.

5- التوافق مع اللوائح: يمكن استخدام AI لأتمتة عمليات الامتثال وتقليل الأخطاء البشرية في التقارير والتدقيق.

6-تكنولوجيا البلوكتشين: قد يتم دمج الذكاء الاصطناعي مع تكنولوجيا البلوكتشين لتعزيز الشفافية والأمان في المعاملات المالية.

دراسة تطبيقية على الحالة المصرية

تُعدّ التطبيقات التي أُقيمت في مصر لتعزيز الأمن السيبراني باستخدام تقنيات الذكاء الاصطناعي من أبرز التجارب في هذا المجال، وكان البنك المركزي المصري هو القائد الرئيسي لهذه المبادرات. يُعتبر البنك المركزي المحرك الأساسي لعجلة التطور المصرفي في البلاد، حيث يسعى دائمًا إلى تحقيق أعلى معدلات الكفاءة من خلال استخدام التكنولوجيا المتقدمة.

من خلال أدواره الاستراتيجية، اتخذ البنك المركزي المصري خطوات مهمة في تنسيق الجهود لحماية الأنظمة الإلكترونية على مستوى القطاع المالي فقد تم تأسيس أول مركز مصري للاستجابة لطوارئ الحاسب الآلي للقطاع المالي مما يعزز أنشطة الاستجابة للحوادث السيبرانية بالإضافة إلى تبادل وتحليل المعلومات الأمنية- تماشيًا مع المعايير الدولية، أطلق البنك المركزي "إطار الأمن السيبراني التنظيمي"، الذي يُعتبر الأول من نوعه في مصر- الهدف منه تحسين إدارة الحوادث السيبرانية، وتوضيح السياسات والإجراءات المتعلقة بتبادل المعلومات، وتحديد الجهات المسؤولة عن التنسيق في المسائل الأمنية.

نجحت جهود البنك المركزي المصري في تطبيق المعايير الدولية للأمن السيبراني، حيث حصل مركز الاستجابة لطوارئ الحاسب الآلي (EG-FinCIRT) على اعتماد وعضوية المنتدى العالمي لفرق الاستجابة للحوادث الأمنية (FIRST). أصبح بذلك أول مركز قطاعي معترف به دوليًا في مصر، مما يعكس التزامه بتعزيز جودة الأمن السيبراني في البلاد وتساهم عضوية البنك المركزي في المنتدى في تحسين مؤشر جودة أمن المعلومات على مستوى الدولة، (Global Cyber Security Index) مما يعزز الثقة في الاقتصاد الرقمي ويجذب الاستثمارات الأجنبية. كما يُعزز ذلك من أمان البنية التحتية المصرفية من خلال تطبيق أحدث الأطر والممارسات العالمية.

في عام 2023، نقل البنك المركزي المصري تجربته الرائدة في الأمن السيبراني إلى نظيره الغاني، تأكيدًا على ريادته في هذا المجال على مستوى القارة الأفريقية. جاء ذلك بناءً على طلب البنك المركزي الغاني، بهدف الاطلاع على هيكل وأهداف استراتيجية الأمن السيبراني في مصر، وكذلك حوكمة مركز الاستجابة لطوارئ الحاسب الآلي ودوره في الوقاية من الحوادث الأمنية حيث تعتبر هذه المبادرات علامة فارقة في تعزيز التعاون بين الدول الإفريقية في مجال الأمن السيبراني، وتسلط الضوء على دور البنك المركزي المصري كقائد في هذا المجال.

الموقع الرسمي للبنك المركزي المصري.

الخلاصة والتوصيات

في الختام، أصبح الذكاء الاصطناعي عنصرًا أساسيًا في تعزيز استراتيجيات الأمن السيبراني يساهم في التنبؤ بالتهديدات وسرعة الاستجابة مما يقلل من التكاليف والوقت والجهد ويتيح الوصول إلى أفضل الحلول وقد تم التوصل إلى النتائج التالية:

1-دور حيوي للذكاء الاصطناعي: تلعب تقنيات الذكاء الاصطناعي دورًا لا غنى عنه في تعزيز استراتيجيات الأمن السيبراني، مما يساعد المؤسسات على التصدي للتهديدات بشكل أكثر فعالية.

2-وضع أطر قانونية: من الضروري إنشاء قواعد وأطر تنظيمية وتشريعية لضمان سلامة بيانات العملاء وتعزيز النزاهة بين المؤسسات، مما يخلق بيئة عمل تكنولوجية آمنة.

3- يجب عقد دورات تدريبية مكثفة لجميع العاملين في القطاع المصرفي لفهم وتطبيق تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني بشكل فعال، حيث يمثلون حجر الزاوية لمستقبل القطاع.

4-تطوير القوانين والأخلاقيات: من المهم تطوير القوانين والاطارات الأخلاقية لضمان الاستخدام الأمثل للتقنيات التكنولوجية في جميع المؤسسات، وخاصة في القطاع المصرفي.

التوصيات

1- استخدام الذكاء الاصطناعي لتحسين خطط الاستجابة للحوادث، من خلال تحليل البيانات السابقة وتقديم توصيات فورية للإجراءات الواجب اتخاذها في حالة حدوث خرق أمني.
2- تطوير تقنيات تشفير تعتمد على الذكاء الاصطناعي لتحسين مستوى الأمان في نقل البيانات، بحيث تتكيف خوارزميات التشفير مع التهديدات الحالية.
3- أتمتة عمليات التحقق من الهوية وعمليات التدقيق الأمني باستخدام تقنيات الذكاء الاصطناعي، مما يقلل من الوقت المستغرق في الكشف عن الانتهاكات ومعالجتها.
4- استخدام أدوات الذكاء الاصطناعي لتحليل المحتوى الإلكتروني، مثل البريد الإلكتروني والرسائل، للكشف عن هجمات التصيد الاحتيالي والمحتوى الضار.
5- إنشاء نماذج تنبؤية تقوم بتحليل البيانات التاريخية وتوقع المخاطر المحتملة، مما يمكّن البنوك من اتخاذ تدابير وقائية مبكرة استخدام تقنيات المحاكاة المدعومة بالذكاء الاصطناعي لتدريب الموظفين على كيفية التعرف على التهديدات السيبرانية والتعامل معها بشكل فعال.
6- تطوير أنظمة مراقبة تعتمد على الذكاء الاصطناعي لرصد الشبكات وأنظمة المعلومات بشكل دائم، مما يساعد على الكشف السريع عن الأنشطة غير المصرح بها.

المراجع

- Dambe, S., Gochhait, S., & Ray, S. (2023, November). The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit. In 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE) (pp. 88-93). IEEE.
- Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. EAI Endorsed Transactions on Creative Technologies, 8(28), e3-e3.
- Tom, B., Suchitra, N., Valeria, G., Michelle, L., Sulabh, S., Tom, M., et al. (2018). AI and risk management innovation with confidence. london: Deloitte.
- Villar, A. S., & Khan, N. (2021). Robotic process automation in banking industry: a case study on Deutsche Bank. Journal of Banking and Financial Technology, vol 5 , 71- 86
- "Cybersecurity and Artificial Intelligence: A Comprehensive Guide" (2022)
- "Cybersecurity Essentials" - Cisco Networking Academy
- "Cybersecurity & Infrastructure Security Agency (CISA)"
- كتاب "Social Engineering: The Art of Human Hacking" لمؤلفه **Kevin Mitnick**.حول الهندسة الاجتماعية
- "CISA" (Cybersecurity & Infrastructure Security Agency) حول أمان الشبكات وطرق الحماية من هجمات DDoS
- OWASP (Open Web Application Security Project) - owasp.org
- NIST (National Institute of Standards and Technology) - nist.gov
- Stallings, W. (2017). *Network Security Essentials: Applications and Standards*. 5th Edition. Pearson

- Marvin Minsky (1927–2016) was an American cognitive scientist, mathematician, and a pioneering figure in the field of artificial intelligence (AI). He was a co-founder of the MIT Artificial Intelligence Laboratory (AI Lab) in 1959 and made significant contributions to AI and cognitive science over his long career.
- John McCarthy (1927–2011) was an American computer scientist and one of the founding figures of artificial intelligence (AI). He made a number of pivotal contributions to AI, as well as to computer science and mathematics in general. McCarthy is best known for coining the term *artificial intelligence*, for developing the LISP programming language, and for his work on the theory of machine intelligence.

- كتاب من تأليف ويليام ستالينغز، وهو يعد مرجعًا مهمًا في مجال أمن الشبكات. النسخة الخامسة، التي صدرت في عام 2017، تغطي مجموعة واسعة من المواضيع المتعلقة بأمن الشبكات
- كتاب "Insider Threats in Cyber Security" للكاتب ج. ه. مور (J. H. Moor) يتناول موضوع التهديدات الداخلية في مجال الأمن السيبراني،
- المصري، فرح محمد. (2024). دور الذكاء الاصطناعي في تحسين الأمن السيبراني. مجلة النخبة للدراسات والأبحاث، 3(2).
- الموقع الرسمي للبنك المركزي المصري :

https://www.cbe.org.eg/ar/news-publications/news/2023/05/17/eg-fincirt-acquires-the-accreditation-and-membership-of-the-global-forum-of-incident-response

https://www.cbe.org.eg/ar/news-publications/news/2023/08/10/17/41/the-central-bank-of-egypt-shares-its-pioneering-cybersecurity-experience-to-the-ghanaian-counterpart

HOTLINE
15200
One number to better serve you!

فرع مدينة نصر (الفرع الرئيسي)
العنوان: ٢٢ أ شارع الدكتور أنور المفتي
مبنى طيبة ٤٠٠، ص.ب. ٨١٦٤ القاهرة

ساعات العمل: ٩:٠٠ صباحاً – ٥:٠٠ مساءً
www.ebi.gov.eg

انضم الى صفحتنا
facebook.com/EgyptianBankingInstitute

تابعنا على
twitter.com/EBItweets

انضم الينا
linkedin.com/company/egyptian-banking-institute

شاهدنا على
YouTube Channel: Egyptian Banking Institute (EBI)