Artificial Intelligence: The New Tool For Cybersecurity in Finance

Michael Reifer
Dept. Computer and information Sciences
Towson University
Towson, United States
mreifer1@students.towson.edu

Calvin Basier
Dept. Computer and information Sciences
Towson University
Towson, United States
cbasier1@students.towson.edu

David Oliseh
Dept. Computer and information Sciences
Towson University
Towson, United States
doliseh1@students.towson.edu

***Abstract*— With the advancements of Artificial intelligence (AI), cyberattacks are becoming harder to defend against in the financial world. Many financial organizations are trying to switch toward the use of AI-driven cybersecurity to combat these attacks, which is significantly improving cybersecurity for financial organizations. AI cybersecurity in the financial sector allows organizations to be prepared for incoming attacks. Techniques such as machine learning (ML) using AI can be used for proactive defense in many parts of the financial world. This method is even more beneficial for financial cybersecurity because AI is exceptional at pattern recognition. For example, credit card fraud can easily be detected by AI through learning a person's spending patterns and identifying anomalies. AI is causing cybersecurity in finance to be optimized at a level that it could not reach before. This research will go into the use, benefits, vulnerabilities, and impacts of AI in the financial world of cybersecurity.**

I. INTRODUCTION

The growth of artificial intelligence over the past couple of years has sparked new ideas for cybersecurity. AI-driven cybersecurity allows for the use of automated systems to flag threats instantly. Various methods have been developed, such as machine learning, deep learning, and natural language processing [1].

Artificial intelligence is very good at using data to improve cybersecurity. Using data that has been collected, these AI cybersecurity systems can defend from common attacks and learn to predict new attacks. These AI methods collect data over a period time and use the information to create new walls of defense. This system of defense is very useful because of the various new methods of cyberattacks, many involving AI [2].

Cybersecurity is especially important in the financial field. With the large amounts of personal data constantly being transmitted, cybersecurity methods must be stronger than before. Common cybersecurity methods, such as artificial neural network (ANN), deep learning, and biometrics, can be amplified using artificial intelligence. AI is a double-edged sword in financial cybersecurity because it can be used for both attacks and defense [3]. This paper will further delve into the methods of attack and defense that are improved by AI.

Attacks being improved by artificial intelligence is not ideal, but it is a side effect of growing technology. Attacks are improved by artificial intelligence by allowing them to be automated. Many attacks include learning financial organizations' current protocols of cybersecurity and exploiting them.

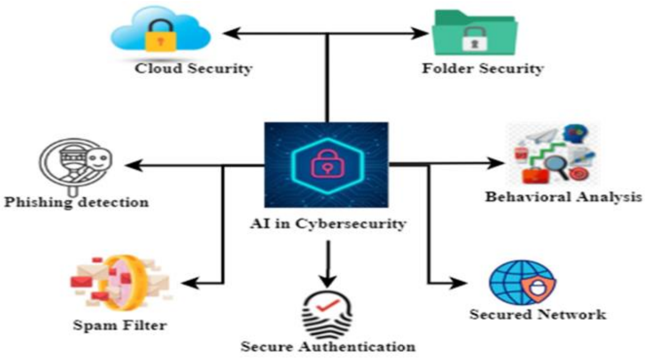

Fig. 1. The use of AI in cybersecurity [4] (not specific to financial institutions).

With the use of currencies online, such as cryptocurrency, new methods of financial cybersecurity are needed. Artificial intelligence is exceptional at finding changes in patterns, and the reliability and accuracy of AI systems makes it a very useful tool for all cryptocurrency exchanges online [5]. With the amount of data that is required to be confirmed in large crypto exchanges – mostly bitcoin – the use of AI is needed more than ever. AI allows data to be protected and transferred very quickly using artificial intelligence defense methods (i.e. machine learning) [6].

Some people who commit malicious scams using bitcoin (or other cryptocurrency) think these scams cannot be tracked. This way of thinking may have been true in the past, but it is not true anymore. Many banks are now switching from traditional methods of cybersecurity to ones which are driven by the use of artificial intelligence. These methods will be investigated further in this paper. The use of artificial intelligence for cybersecurity in the banking industry has significantly helped with identifying money laundering, fraud, and detections of unusual transactions [7].

With all of the talk of AI-driven cybersecurity in the financial sector, this leads us to wonder: what are the bounds of AI-driven cybersecurity? Since this form of cybersecurity is very new to the banking industry, there are many unknown variables. The presence of unknowns can make it hard for many banking companies to successfully implement artificial intelligence as a tool for cybersecurity. Often times, the difficulty lies in understanding how artificial intelligence can be applied to a current cybersecurity protocol [8][9]. This issue limits the amount of organizations that can use these new AI-driven methods.

Many people may think that the widespread reach of AI-driven cybersecurity means that AI can fully replace humans in financial cybersecurity. However, this fallacy is far from the truth. AI could reduce the amount of concerns a human has to consider, but it will not eliminate the use of humans [10]. Many attacks are currently made to specialize in disrupting AI-driven cybersecurity, and these kinds of attacks will not stop any time soon.

The objective of this paper is to examine the methods used in financial cybersecurity that pertain to artificial intelligence. Many survey papers focus heavily on the AI-driven methods of defense in the financial sector, neglecting to cover the methods of attacks. In addition, there are very few surveys that go into detail about the methods of AI-driven attacks in the financial sector. However, the number of publications regarding the use of AI in the financial sector has increased in the last couple of years [11], showing the growth of AI in financial cybersecurity. Through the utilization of recent research, this paper will equally look at both the methods of defense and attacks using AI.

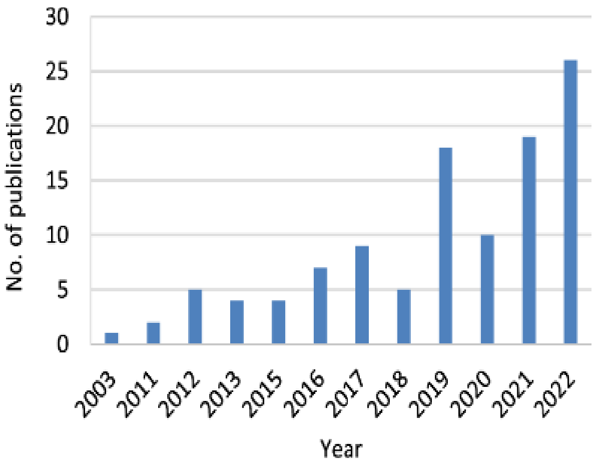

Fig. 2. The number of publications regarding the use of AI in financial cybersecurity [11].

This paper is structured into four sections. The second section will do a deep dive into the methods used for attacks against the financial sector of cybersecurity. This section will go over how these new advancements of artificial intelligence technology are used maliciously. The third section will go over the defense methods that are used in the financial sector to ward off the attack methods that were discussed in section two. This section will also mention the challenges and weaknesses that financial organizations face when using these new AI-driven methods. The fourth section will cover the impacts of using these AI-driven cybersecurity methods for financial institutions.

II. AI Methods Used for Attacks in Cybersecurity in Fianance

A. *Overview*

As mentioned before, AI is making a big impact on the entire world. Focusing solely on the financial sector, AI is both a great tool that can be utilized to help defend against the current ongoing threats but also lead the charge as the perpetrator of attacks. Before we delve into the subject, we have to fundamentally understand the current need for it in the first place. Firstly, cybercrime, by definition, is “the use of computer technology or online networks to commit crimes” [12]. According to Fischer [13], cybercrime can cost the global economy upwards of 400 billion dollars. Other reports show it is increasing to trillions [14]. These attacks are motivated by a variety of things, like, for example, financial gain, politics, and espionage [15]. There are a plethora of cybercrimes that plague the financial field, but they can now be enhanced by the use of AI, and this section will go into detail about a few to be aware of and how they work.

B. *Methodoligies*

Adversarial attacks on machine learning: Adversarial machine learning is a subset of machine learning that specializes in studying machine learning attacks [16][17]. In the financial context, machine learning is present in multiple ways, like Fraud detection, Robo-advising, credit scoring, anti-money laundering detection, chatbots, payment-transaction monitoring, and a lot more [17][18]. Adversarial attacks against machine learning models (ML) present a concerning issue on the sanctity of the outputs these models produce in the automation of their tasks. Any confidential information within these models is at risk of being tampered with or stolen by cybercriminals if not properly defended [17]. The general functions of adversarial attacks go as follows: Poisoning is an attack on machine learning models in which the attacker aims to input data into the model to “Learn the wrong way” [17]. In addition, we have Evasion attacks, which are attacks on machine learning models that aim to confuse the model by editing something about input data in order to confuse and create a misclassification [17]. Lastly, Extraction attacks are attacks that aim to “reconstruct, or extract” information about the model, like how it was trained or information about the data it uses [17].

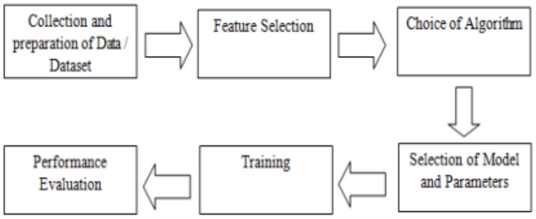
Collection and preparation of Data / Dataset
Feature Selection
Choice of Algorithm
Selection of Model and Parameters
Training
Performance Evaluation

Fig. 3. Figure of Generic ML model components [19] (not specific to financial institutions).

Attacks can be classified as either indiscriminate or targeted. Indiscriminate attacks try to degrade the value of the entire system, ignoring types of instances affected and simply pursuing its goal [20]. Targeted attacks do as the name implies and focus on a specific component or aspect of the AI system with the intention of either degrading performance, like mentioned before, or creating privacy attacks on the training component of the model [20]. In evasion attacks, one of the new methods is by utilizing GAN's (Generative Adversarial Networks) and DNN's (Deep Neural Networks) to create adversarial samples. They achieve this by using two models in which one generates samples, then the other discriminates which ones are fakes until they can reach a perfect balance, producing adversarial samples that they can sneak inside the target's pre-trained DNN or GAN [20]. In Poisoning attacks, the same method can be used to create adversarial samples, but the goals are different [20]. Poisoning attacks instead happen during the training phase of the ML model for it to learn incorrectly and develop a bias towards the malicious samples [20]. By doing this, the adversary teaches the model to label the incorrect data as correct from the start, creating a functionally useless model [20]. The requirement for this is that the attacker has some form of access to the training and testing datasets, respectfully [20].

Ai Powered Malware: Malware itself is malicious software or programs made with the intention of "disrupting, altering, or destroying" the critical functions of computers, networks, and devices [21]. With new advancements within machine learning/deep learning, new malware is being produced by cyber attackers that allow it to learn from its environment and modify and update itself as time goes along, whilst producing variants of itself [22]. AI's usage in malware can be utilized in many ways, for example, hiding malware code from detection in DNN's (Deep Neural Network) [23]. In evasion attacks, the malicious users sneak their malicious data past detection from an ML's classifying components. In this situation, the data is malware code with the intention of doing several malicious actions against ML systems [23].

Malicious botnets are collections of host PC's controlled by a singular entity [24]. In the past, Anti-viruses and IDS's (Intrusion Detection Systems) both detected malware and malicious botnets by scanning for known behavioral patterns [24]. The malware would bypass this by using packers, a software to compress and conceal the malware [24]. The new method uses evolutionary packers that use a Turing-complete evolutionary algorithm that, in turn, makes entirely new algorithms. The encoding and decoding process is now randomly generated and built into the malware itself [24].

Ai Powered Social Engineering Attacks: Phishing is the fraudulent act of obtaining sensitive user information, such as login information, credit card/banking information, money, and more through a series of text messages, emails, phone calls, and other forms of communication that act as real, legitimate organizations or individuals but really are not [25][26]. Typically, this is done through the preferred communication method the attacker uses but with a malicious attachment or fake URL [25]. Specialized attacks like business email compromises (BEC) utilize phishing on a larger, more advanced scale to coordinate attacks on financial institutions, businesses, and individuals by tricking them into wire transfers [26]. This form of phishing was reported as the second most costly in 2023 by the internet crime complaint center at 2.9 billion dollars [26]. Now, newer methods are available to help empower these scams through Generative AI, a new subset in machine learning that can create various forms of content with human characteristics, like image generation, video generation, natural language generation, and more [27]. These advancements can be utilized to create new malicious emails/ phishing attacks at a faster rate due to automation [27].

Ai-Password Attacks: Passwords are one of the commonly used authentication methods within cybersecurity [28][29]. The wide use of this method is mainly due to it being easy to implement and easy to adopt for most users [29]. Due to passwords being so easy to adopt and a widespread method, they are also exploitable because each service or software using this method has different requirements [29]. With human memory being limited, each user must mentally juggle multiple passwords for each service, causing them to build weaker passwords for the sake of memory over protection [29]. This effort solves the major problem of memorizing their passwords but at the cost of security and opens users up to password attacks [29]. Currently, the old methods are being flipped due to AI being introduced, creating newer and more sophisticated attacks [28][29]. For instance, one of these attack methods involves using generative adversarial networks to generate password guesses [28]. With this research method proposed by Hitjal et al., their method, PasGAN, uses deep learning to generate password guesses [28]. Its base includes the same concepts that were previously discussed, using generators and discriminators but to train them to understand characteristics of passwords After going back between each other, eventually the result is a password guesses that can be used in attacks until they breach an account [28]. Furthermore, this leaked password can be imputed and used to further train the model and be used to create more accurate guesses, becoming an even bigger threat [29].

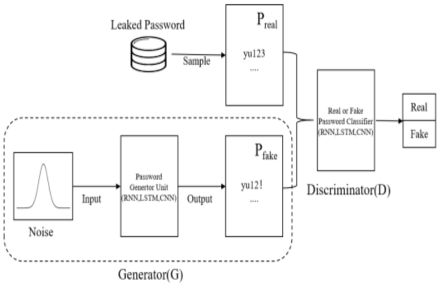

Fig. 4. Illustration of GAN password guessing model [29].

C. *Challenges and Perspectives*

So far, we have discussed in brief how Adversarial attacks, AI-Powered Malware, AI-Powered Social Engineering attacks, and AI-powered Password Attacks all are methods that can be used in attacks. The focus has not been too much on financial institutions, businesses, or individuals, but all of these can overlap and become threats in one way or another. For financial institutions, if they use a Machine learning model in any context for things like financial trading or fraud detection, they are susceptible to an attack on the model and must be on the top of their game in defenses to ensure their model is accurate and secure.

In the same sense, Social Engineering attacks are a big problem for financial institutions for the fact that they are not always technical. We currently use a system of numeric values to score potential risks when doing risk assessment for cybersecurity; we factor in real world observations and data to get a general understanding of the value of the information [30]. The issue is the uncertainties that we cannot calculate, like human error and evolving/emerging threats [30]. We have gone into detail about the emergence of new AI-assisted or empowered attacks that both act as these uncertainties. The issue is clear, and the only way to move forward is to develop strategies or update our current defenses to mitigate the risk and bolster defenses.

For social engineering and phishing attacks, something I believe we need to see is in-depth detection methods that further catch new trends. Better email filtering and onsite training between corporations and institutions could be a step in the right direction for further driving down the risk by having competent users who know what they are doing and are more likely to not fall for these traps. For BEC crimes, I believe that we need to develop a better form of authentication within the chain of command to really drive down this area's influence. Social engineering and phishing attacks are a big area of influence within the financial sector because of the high importance it has as a critical infrastructure. At the same time, I can recognize that all of this is in an area of uncertainty because human error plays a good part in it. Although, I still believe that if we can further address and come up with new ideas, we can help lessen it more and more, so it does not have such a high percentage on cybercrime.

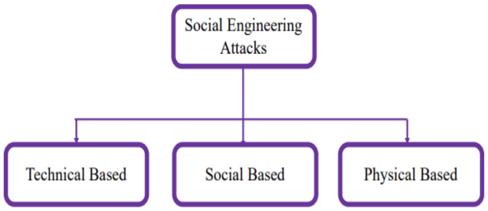

Fig. 5. Social Engineering attack types [31].

For the case of malware, this area is deep and has a lot of applications of malicious programs that are further increasing as AI progresses more and more. AI is a tool for us that can be utilized to help defend against these attacks, but at the same time, it acts as this problem because just as much as we develop and progress, our adversaries find new, creative ways to utilize the new resources. We play a constant game of tug-of-war with innovation, and it is an uncertainty, like stated before, that we cannot control; however, what we can do is our best to mitigate it by being up to date on how it is being utilized and doing our best to create better defenses and accurate defenses. Adversarial attacks are one of the areas that I feel the game of tug-of-war is the most prevalent because of machine learning's applications being able to be utilized by the same people we are fighting. It creates this relationship of needing to ensure models are accurately doing their job whilst also dealing with threats that can turn them useless, like poisoning attacks, as mentioned before. I believe we have to be extremely careful in this department to ensure that we monitor machine learning models because of the fact that adversaries are taking advantage of making them biased towards their malicious samples or malware or stealing confidential data out of them entirely. The battle between ensuring that we are up to date and aware of the concerns of the attacks is extremely important.

For password attacks, just like social engineering, I believe our best approach for dealing with these attacks is, again, keeping our detection tools (our machine learning models) functioning and, once again, adopting new methods for prevention. Password policies are hard to deal with, and that is a given with how widespread these policies are, in combination with our issues with retaining them. That is why I think moving onto other authentications, specifically for finance, is a better alternative than passwords. Utilizing biometrics, for example, might be a good way to help, even if it is costly. I am aware it might not be foolproof or cost effective entirely, but having more than one authentication method would probably do us much better than having to retain passwords constantly and running the same game of human error due to lack of memory for each individual service we use.

Finance is a more important industry when it comes to our lives, though, and I think taking the investment would do a much better job at cracking down on password attacks plaguing us. Outside of replacing them or adding to them – which, again, I understand might not be doable – I believe we should keep doing what we are with adversarial attacks to prevent tampering of machine learning models. The goal is to protect the datasets and keep them confidential, ensuring that they are not biased or compromised in order to utilize the new technology we have before us.

Overall, we recognize the issues currently surrounding AI-based cyberattacks in multiple different areas, using a wide array of tactics utilizing new developments within machine learning and more. As the financial sector identifies all the new sophisticated or automated methods of AI, it is extremely important to utilize it as a tool in the same way. As stated again and again, it is like a tug-of-war, but AI can still be used in many ways to improve our defenses and continue to be a useful tool in general for efficiency, automation, and decision making. In the following section, we will investigate a variety of methods AI can utilize in defending our systems and how the financial world should utilize it as a powerful tool of defense. We will also again look at shortcomings, but with optimism on how they can be mitigated and improved. In closing, we should keep our systems secure and continue to record and note the emerging trends within AI-based attacks to ensure our adversaries are not profiting as much in the game as we are off all the positives AI can bring to our lives.

III. METHODS USED IN DEFENCE FOR CYBERSEUCIRTY IN FIANACE

A. Overview

The development of AI has resulted in increasing methods for attacks on the finance sector, but it also has increased the defense part of it. There are many new methods that have been developed, like Artificial neural networks (ANNS) and artificial immune systems, in addition to other methods [32]. This part of the paper serves to inform and talk about the methods that AI facilitates in order to create stronger defense systems from the methods of attacks being made to the finance sector.

Threats in finance: There are many methods of attacks that can take form in the realm of cybersecurity. These attacks can cause threats to the financial sector. Some of these attack methods include the following:

Phishing attacks: This type of attack is a big threat against online banking because it can cause major losses in the financial sector. These losses can include both the loss of finances and also a loss of data [33].

Cyber espionage: Espionage is taking information from the owner without their permission – in plain terms, stealing. The method of cyber espionage is used when the perpetrators launch an attack on a financial company for the sake of money or economic gain [34].

Machine Learning: The financial sector has been growing, which means there are going to be more attacks on the finance industry [35]. The finance industry has been investing in machine learning algorithms in order to protect their assets and data. In the finance industry, there have been ups and downs. The role of machine learning is to analyze where there was success, find out why it was successful, and take that data collected to be able to predict and explore other options.

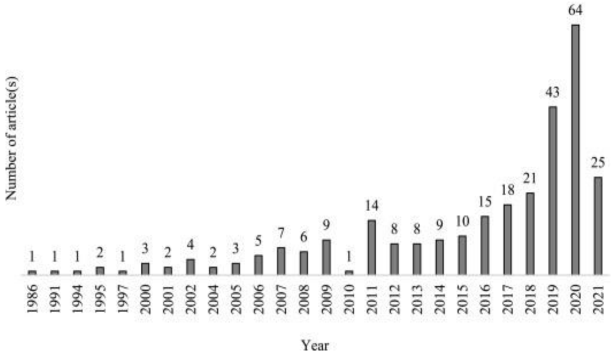

Fig. 6. Increase in articles from the use of machine learning in cybersecurity (not specific to financial sector) [35].

AI Methods Used for Defense:

Artificial Neural Network (ANNs): ANN's are made of different layers of nodes that help move information between the input nodes and the output nodes [32]. ANN's are an example of soft computing methodologies because they are able to copy biological neural networks. This method has three different nodes that have different options. Firstly, there is an input layer node whose function is to take in the data that is being inputted. There are also hidden nodes that are usually located in between the input layer and the output layer of the network. They play a crucial role in enabling whatever function is being inputted inside the network. Lastly, the output nodes are called the final layer of the network because it produces the output. The job of these nodes is to change the value into a suitable and comfortable format. This technology is currently one of the methods used as a defense in these ways [36].

Credit Card Fraud Detection: Credit card fraud happens when someone steals a credit card and tries to use it without authorization [37]. Without the proper defense method, this could be a big problem for both the company of the credit card and the customer of the company. In order to combat this kind of fraud, companies put in the ANN's so that this defense mechanism can detect against fraud. The fraud detection is activated as soon as the customer inputs the necessary information or password to be able to use the credit card. ANN's put the information through a test to see if it falls under the fraud category or non-fraud category [38].

Risk management: This idea relates to companies making decisions in order to help their company grow [39]. ANN's have the ability to grow because they are such a self-learning machine that is able to read patterns and identify any potential risk that may come up in the future. This is a good way to protect the company's future by being able to provide the different types risks of every different option that the company wants to take.

Credit Scoring: The ANN's algorithms are used to make performance peak. ANN's, in this scenario, are being used to see if any credit applicants are able to get accepted based on their current payment history. They can also predict one's credit behavior. This is very important for credit card companies so that they do not just accept anybody. With the use of ANN's, these companies are able to detect if people deserve to be accepted into their programs or not [40].

Network Intrusion Detection Using Deep Learning: This is where we start to apply the use of different neural networks like CNN's, RNN's, and others to provide some sort of defense to the finance sector [41].

NIDS: The NID's are important because they have the ability to detect unusual traffic flows, in addition to unauthorized access [42]. Another one of their abilities is being able to deep learn; they can use past ways from attackers and learn from them so that they would be able to detect what an attacker is like. NID's are a good way to help companies defend against any attackers that want to attack their financial sector by having a tiki-taka framework. Having a tiki-taka framework increases the defense and resistance to any attacks. Some of the examples of NID's are snort, Suricata, and IBM QRadar.

Generative Adversarial Networks (GAN's): GAN's are made up of two neural networks called a generator and a discriminator [43]. Using GAN's in finance would lead to many developments in in the financial sector. They are also part of the deep learning techniques that help improve financial data. They are able to learn the financial time series that helps financial companies take the least risk [44].

Behavioral Biometrics Systems: Behavioral biometrics is one of the AI defense methods available to cybersecurity. It provides an alternate method, unlike the normal authentication methods, like passwords or pins [45]. The behavioral biometrics method studies the user's behavior. Through this process, the system is able to tell when a threat is near and can provide appropriate security measures.

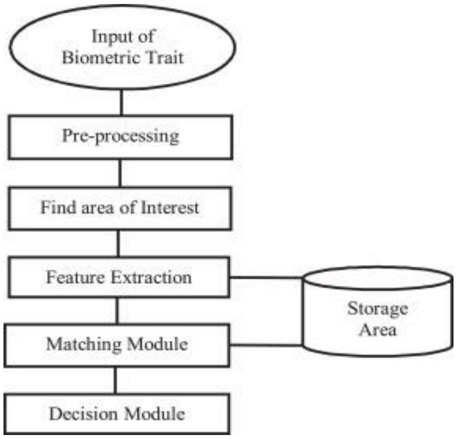

Fig. 7. How a biometric system works (not specific to financial institutions) [45].

Integration XAI - Based Techniques – Phishing attacks have been one of the famous ways that attackers use to deceive a user into getting their information [46]. One of the ways cybersecurity has to defend against this type of attack is to utilize integration XAI-based techniques. These techniques can provide information on how AI thinks and is able to process information in order to predict outcomes. They also have the ability to be able to tell the weakness and also the strengths of each AI-based model.

B. Challenges and perspectives

There are strong AI-based defense mechanisms that help the finace sector, but they also have their weakness. However, the progress that has been made by AI-based defense is increasing rapidly. The development of cybersercurity that continues to unfold toward the attacks made against the financial sector is very impressive, but I also think it can improve in a number of ways.

There are many threats and failures that could occur when we involve AI-based defense in cybersecurity regarding the finance sector because AI can also make mistakes. On the other hand, I also think it can be a great asset based on how well it is able to adapt to different types of threats and to learn from past events. The ability of AI to adapt and learn can make it a better tool overall. This feature also makes it unique because it is more advanced than other methods of defense, with the benefit of all the information that it is able to acquire.

Phishing Attacks: Cybersecurity defenses have taken a lot of attacks, but phishing attacks are one of the most famous types of attacks; they are also the hardest to combat since they have to do with one's identity being stolen. In my opinion, I think there should be a way that we can bolster our defense mechanisms enough to avoid these types of attacks so that, in the future, there is less personal information stolen and fewer casualties. I think that using AI is going to be a good way of accomplishing this goal, and it might also be the only way to combat against this type of attack. If we had the capacity to improve AI to the point that it could perfectly differentiate between users, that would be ideal. It would be worthwhile to evolve AI to have the functionality to determine whether a user is legitimately trying to get into their account or whether it is someone trying to use their identity to apply for something.

However, AI also has its flaws. In the same way that all computers can make mistakes, AI can also make mistakes. One of the ways I think we can combat this type of attack is by creating some type of camera access AI. A drawback to this idea is that some users may see this defense mechanism as an invasion of privacy. In this manner, we can think about how face IDs on the iPhone work with the way they are able to detect certain points on a person's face. Through that mechanism, the phone technology is able to detect if the person attempting to unlock the phone should have access to whatever the user is trying to do. If we were to mimic that method of camera access AI (which we could probably easily make), it could change things around. If there were an issue with access, the option would be available to get a raw data live feed from wherever the person is accessing the account. Whoever is trying to use the stolen identity could be compared to what the actual person or owner looks like. With this type of defense it would be a lot harder for people to steal identities, and there would be fewer causalities from these types of attacks.

In conclusion, I believe if we were to add some identity methods that allow the owners to able to access their accounts (or whatever they need their identify for), the finance cybersecurity would be a lot stronger than it already is. However, the downside to this type of defense that we've proposed is that it may not be the most ethical way of solving this problem because there could be many implications and also lawsuits that could probably come from various issues; therefore, it is best to make sure the user signs a terms and agreement policy before this procedure is put in place. Lastly, with the data we get from this method of defense, this can also be used to further improve the accuracy of AI defense regarding the phishing attacks [47].

Credit Card AI: Credit card-AI that has been able to detect abnormal use of someone's credit card that is different from the owner of the credit card is very impressive. There has been an improvement in this side of cybersecurity with there being fewer thefts and less money stolen. However, I personally think that this area still has room for improvement.

Yes, it is harder to be able to access someone's credit card, yet, at times, I also think that it can be easier based on my own personal experience. I remember, when my mom would give me her credit card to go to the store to buy her stuff, I was able to access her credit card so easily without even knowing the pin, all by pressing the green button when the charges had come up. This is to show how easy it could be for an unauthorized person to be able to get your credit card and be able to use it, even without the correct password or pin.

As said in the article "Inconsistencies in big data," we can see some of the challenges that come with battling credit card fraud, some of them being financial losses for the stakeholders [48]. It is the job of cybersecurity to be able to have a way to tell if one is a fraud or not. I also think that using machine learning methods to be able to tell if there is a credit card fraud attempt has been helpful, so far. These methods have been successful since they are able to analyze how the original owner of the card spends; by comparing previous spending habits to current spending, they can see if there was an abnormal amount of money being used out of nowhere. This method is a good start, but I also think that it is not enough because so many things can go wrong, especially with AI. AI is not perfect, but it improves in accuracy with every case.

One of the ways I think we could fight against the downfalls of AI is to add some help to AI via human assistance. This would work by us humans helping the AI in all facets. Working together with AI would help with being able to tell if there is suspicious activity going on with the credit card. This activity can be assessed by monitoring the locations at which items were purchased; if there is any possible suspicious activity, humans can contact the customer with an automated voice, asking if they had made the purchase in question. With this type of proposed method, we could combat credit card fraud: the rate of credit card fraud would be lowered by working together – a combined effort between humans and AI. Despite all the problems and improvements that could be made, I still think the progress made by AI-based defense is beneficial and impressive.

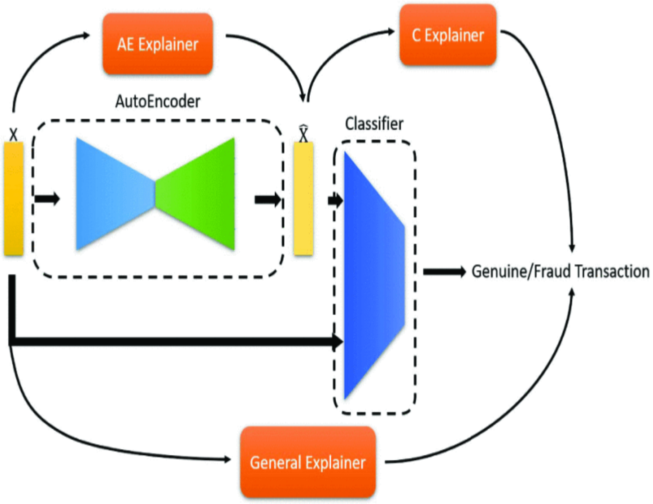

Fig 8. Credit card fraud model for AI [49].

Credit Scoring: Credit scoring has been one of the most important aspects of our modern life because we need a good credit score to be able to obtain necessities for having a sustainable life; some of these necessary things include cars and houses [50]. Since it is really important to have a good credit score to be able to purchase necessities, we need to make sure the method for calculating credit scores is executed properly. This execution will make sure people's credit scores reflect reality so that those who deserve a good credit score will actually receive a good credit score and those that do not deserve a good credit score do not accidentally end up having a good credit score.

The AI we use that is called ANN is used to check people's backgrounds to see if they deserve a credit card or not. This type of technology also has a lot of data inconsistencies because of how much big data it is bringing in [51]. By updating and developing the ANN AI, we can smooth out the inconsistencies and build a more dependable technology. It would also be worth looking into the use of other AI technologies to solve some of the downfalls of ANN in credit scoring.

IV. Conclusion

This paper has laid out the foundations of AI-driven cybersecurity in the financial sector and has provided information on the attacks and defenses in the financial sector that are driven by AI. We have provided a survey that combines information from many papers that have researched the use of AI-driven cybersecurity in the financial field. Some challenges of incorporating AI-driven cybersecurity systems were mentioned, including how, in our opinion, these challenges can be mitigated. Also, an insight into AI attacks was provided, in addition to how they can be dangerous to financial organizations. Since AI-driven cybersecurity in finance is so new, there are many potential applications that can be explored in the future, which we do not yet know about.

These new methods for cybersecurity in the financial sector using AI will continue to become more widely used across the field. These methods allow for cybersecurity workers to focus more on the things which cannot be automated by AI. AI will continue to improve, and, eventually, all cybersecurity needed for the financial sector could be automated. This does not mean that humans will be removed from cybersecurity in the financial sector. Since AI has weaknesses, there will always be a use for humans in cybersecurity for finance. The new attacks formed because of the use of AI are dangerous and should be considered by financial organizations before switching from traditional cybersecurity methods. Though this should be considered, financial organizations should start switching to AI-driven methods for cybersecurity. If the majority of organizations continue to adopt AI, it will continuously improve.

The impact of AI-driven cybersecurity in the financial sector will continue to be researched as these methods continue to be developed and used. So far, we see an increase in credit card detection fraud and anomaly detection. AI has had a positive impact in the financial sector of cybersecurity. It has caused many elements of cybersecurity in the financial sector to be automated. It also improves the existing structure of cybersecurity for financial organizations.

However, AI has also created a lot of challenges for financial organizations. Many of these challenges are resulting from all of the new attacks, which are able to be automated and dig deep into the weaknesses of a financial organizations' cybersecurity. For example, Adversary Machine Learning (AML), a method discussed in this paper, spins AI into a deadly tool to financial companies' assets. We already see the use of AI-driven cybersecurity attacks on financial organizations. Many times, these attacks will be the most successful ones, resulting in the largest payouts for criminals. AI-driven cybersecurity attacks in the financial field are also harder to defend against because AI is constantly evolving.

There is a large gap in research of AI-driven systems in the financial field. Many publications include research of AI-driven cybersecurity but not in the financial sector. Information on cybersecurity attacks in the financial field using AI is hard to find. This is because, usually, there will not be research done on these attacks until they happen. In the future, more publications regarding the use of AI-driven cybersecurity in the financial sector will continue to be published. More information has to be released on the methods of attacks using AI in the financial field to better financial organizations' cybersecurity.

For the future, it seems that AI will become dominant in the financial sector of cybersecurity. With new advancements, AI cybersecurity is constantly pushing the boundaries further and further; the future is AI-driven cybersecurity in finance. Machine learning is already very dominant in financial organizations to better their defenses, and the addition of other AI methods will further bolster cybersecurity in the financial sector. We will continue to see more methods become common. The methods of defense mentioned in this paper are just the start of AI-driven cybersecurity in finance.

References

[1] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," *SN Computer Science*, vol. 2, no. 3. Springer, May 01, 2021. doi: 10.1007/s42979-021-00557-0.

[2] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, "Weaponized AI for cyber attacks," *Journal of Information Security and Applications*, vol. 57, Mar. 2021, doi: 10.1016/j.jisa.2020.102722.

[3] K. AL-Dosari, N. Fetais, and M. Kucukvar, "Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges," *Cybernetics and Systems*, vol. 55, no. 2, pp. 302–330, 2024, doi: 10.1080/01969722.2022.2112539.

[4] S. Mishra, "Exploring the Impact of AI-Based Cyber Security Financial Sector Management," *Applied Sciences (Switzerland)*, vol. 13, no. 10, May 2023, doi: 10.3390/app13105875

[5] T. Choithani, A. Chowdhury, S. Patel, P. Patel, D. Patel, and M. Shah, "A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking System," *Annals of Data Science*, vol. 11, no. 1, pp. 103–135, Feb. 2024, doi: 10.1007/s40745-022-00433-5.

[6] F. Sabry, W. Labda, A. Erbad, and Q. Malluhi, "Cryptocurrencies and artificial intelligence: Challenges and opportunities," *IEEE Access*, vol. 8, pp. 175840–175858, 2020, doi: 10.1109/ACCESS.2020.3025211.

[7] M. Thisarani and S. Fernando, "Artificial intelligence for futuristic banking," in *2021 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2021 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Jun. 2021. doi: 10.1109/ICE/ITMC52061.2021.9570253.

[8] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, "The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review," *IJARCCE*, vol. 11, no. 9, Sep. 2022, doi: 10.17148/ijarcce.2022.11912.

[9] A. R. D. Rodrigues, F. A. F. Ferreira, F. J. C. S. N. Teixeira, and C. Zopounidis, "Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven

framework," *Research in International Business and Finance*, vol. 60, Apr. 2022, doi: 10.1016/j.ribaf.2022.101616.

[10] A. Mehrotra, "Artificial Intelligence in Financial Services – Need to Blend Automation with Human Touch," *IEEE Xplore*, Apr. 01, 2019. https://ieeexplore.ieee.org/abstract/document/8776741

[11] E. R. Ndukwe and B. Baridam, "A Graphical and Qualitative Review of Literature on AI-based Cyber-Threat Intelligence (CTI) in Banking Sector", *EJENG*, vol. 8, no. 5, pp. 59–69, Oct. 2023.

[12] J. Hawdon, "Cybercrime: Victimization, Perpetration, and Techniques," American Journal of Criminal Justice, vol. 46, no. 6. Springer, pp. 837–842, Dec. 01, 2021. doi: 10.1007/s12103-021-09652-7.

[13] E. A. Fischer, "Cybersecurity Issues and Challenges: In Brief," 2016. [Online]. Available: www.crs.gov

[14] Usaid, "Why Does Cybersecurity Matter for EGAT? Cybersecurity ECONOMIC GROWTH AND TRADE (EGAT) KC Nwakalor for USAID / Digital Development."

[15] N. Tariq, "Journal of Internet Banking and Commerce IMPACT OF CYBERATTACKS ON FINANCIAL INSTITUTIONS," 2018. [Online]. Available: http://www.icommercecentral.com

[16] K. J. Burns, M. Hadjimichael, A. D. Molina-Markham, and J. T. Sexton, "A Taxonomy and Terminology of 3 Adversarial Machine Learning", doi: 10.6028/NIST.IR.8269-draft.

[17] A. Rubtsov, "FINANCIAL INNOVATION SERIES Adversarial Machine Learning: Risks and Opportunities for Financial Institutions FINANCIAL INNOVATION SERIES | Adversarial Machine Learning: Risks and Opportunities for Financial Institutions 2 Global Risk Institute," 2022. [Online]. Available: https://arxiv.org/

[18] V. D. Soni, "ROLE OF ARTIFICIAL INTELLIGENCE IN COMBATING CYBER THREATS IN BANKING." [Online]. Available: www.iejrd.com

[19] J. Alzubi, A. Nayyar, and A. Kumar, "Machine Learning from Theory to Algorithms: An Overview," in Journal of Physics: Conference Series, Institute of Physics Publishing, Nov. 2018. doi: 10.1088/1742-6596/1142/1/012012.

[20] K. Heinrich, J. Graf, J. Chen, and J. Laurisch, "Fool me Once, Shame on you, Fool me Twice, Shame on me: A Taxonomy of Attack and Defense Patterns for AI Security," 2020. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS45481219

[21] A. Djenna, A. Bouridane, S. Rubab, and I. M. Marou, "Artificial Intelligence-Based Malware Detection, Analysis, and Mitigation," Symmetry, vol. 15, no. 3, Mar. 2023, doi: 10.3390/sym15030677

[22] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, and V. Pospelova, "The Emerging Threat of Ai-driven Cyber Attacks: A Review," Applied Artificial Intelligence, vol. 36, no. 1. Taylor and Francis Ltd., 2022. doi: 10.1080/08839514.2022.2037254.

[23]]E. Zouganeli, A. Yazidi, G. Mello, and P. Lind, Eds., Nordic Artificial Intelligence Research and Development, vol. 1650. in Communications in Computer and Information Science, vol. 1650. Cham: Springer International Publishing, 2022. doi: 10.1007/978-3-031-17030-0.

[24] M. Gaudesi, A. Marcelli, E. Sanchez, G. Squillero, and A. Tonda, "Malware obfuscation through evolutionary packers," in GECCO 2015 - Companion Publication of the 2015 Genetic and Evolutionary Computation Conference, Association for Computing Machinery, Inc, Jul. 2015, pp. 757–758. doi: 10.1145/2739482.2764940.

[25] .European Union Agency for Cybersecurity, Phishing ENISA Threat Landscape January 2019 to April 2020, ENISA, 2020. [Online]. Available:https://www.enisa.europa.eu/publications/phishing/view/++widget++form.widgets.fullReport/@@download/ETL2020+-+Phishing+A4.pdf. [Accessed: 2-May-2024]

[26] Federal Bureau of Investigation, Internet Crime Report, 2023. [Online]. Available:https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf. [Accessed: 2-May-2024].

[27] P. V. Falade, "Decoding the Threat Landscape : ChatGPT, FraudGPT, and WormGPT in Social Engineering Attacks," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, pp. 185–198, Oct. 2023, doi: 10.32628/cseit2390533.

[28] B. Hitaj, P. Gasti, G. Ateniese, and F. Perez-Cruz, "PassGAN: A Deep Learning Approach for Password Guessing," Sep. 2017, [Online]. Available: http://arxiv.org/abs/1709.00440..

[29] W. Yu et al., "A Systematic Review on Password Guessing Tasks," Entropy, vol. 25, no. 9. Multidisciplinary Digital Publishing Institute (MDPI), Sep. 01, 2023. doi: 10.3390/e25091303.

[30] A. Fielder, S. König, E. Panaousis, S. Schauer, and S. Rass, "Risk assessment uncertainties in cybersecurity investments," Games, vol. 9, no. 2, Jun. 2018, doi: 10.3390/g9020034.

[31] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," Future Internet, vol. 11, no. 4. MDPI AG, 2019. doi: 10.3390/FI11040089. .!

[32] K. AL-Dosari, N. Fetais, and M. Kucukvar, "Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges," *Cybernetics and Systems*, vol. 55, no. 2, pp. 302–330, 2024, doi: 10.1080/01969722.2022.2112539.

[33] Adedoyin Tolulope Oyewole, Chinwe Chinazo Okoye, Onyeka Chrisanctus Ofodile, and Chinonye Esther Ugochukwu, "Cybersecurity risks in online banking: A detailed review and

[34] M. Button, "Editorial: economic and industrial espionage," *Security Journal*, vol. 33, no. 1. Palgrave Macmillan Ltd., Mar. 01, 2020. doi: 10.1057/s41284-019-00195-5.

[35] J. W. Goodell, S. Kumar, W. M. Lim, and D. Pattnaik, "Artificial intelligence and machine learning in finance: Identifying foundations, themes, and research clusters from bibliometric analysis," *Journal of Behavioral and Experimental Finance*, vol. 32. Elsevier B.V., Dec. 01, 2021. doi: 10.1016/j.jbef.2021.100577

[36] K. T. Yang, "Artificial Neural Networks (ANNs): A new paradigm for thermal science and engineering," *Journal of Heat Transfer*, vol. 130, no. 9, Sep. 2008, doi: 10.1115/1.2944238.

[37] A. RB and S. K. KR, "Credit card fraud detection using artificial neural network," *Global Transitions Proceedings*, vol. 2, no. 1, pp. 35–41, Jun. 2021, doi: 10.1016/j.gltp.2021.01.006.

[38] A. Xu, H. Chang, Y. Xu, R. Li, X. Li, and Y. Zhao, "Applying artificial neural networks (ANNs) to solve solid waste-related issues: A critical review," *Waste Management*, vol. 124. Elsevier Ltd, pp. 385–402, Apr. 01, 2021. doi: 10.1016/j.wasman.2021.02.029.

[39] S. K. Chandrinos, G. Sakkas, and N. D. Lagaros, "AIRMS: A risk management tool using machine learning," *Expert Systems with Applications*, vol. 105, pp. 34–48, Sep. 2018, doi: 10.1016/j.eswa.2018.03.044.

[40] D. Soydaner and O. Kocadağlı, "Artificial Neural Networks with Gradient Learning Algorithm for Credit Scoring." [Online]. Available: http://dergipark.ulakbim.gov.tr/iuisletme

[41] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, Feb. 2018, doi: 10.1109/TETCI.2017.2772792

[42] C. Zhang, X. Costa-Perez, and P. Patras, "Tiki-Taka: Attacking and Defending Deep Learning-based Intrusion Detection Systems," in *CCSW 2020 - Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop*, Association for Computing Machinery, Inc, Nov. 2020, pp. 27–39. doi: 10.1145/3411495.3421359.

[43] F. Eckerli and J. Osterrieder, "GENERATIVE ADVERSARIAL NETWORKS IN FINANCE: AN OVERVIEW A PREPRINT," 2021. [Online]. Available: www.cost.eu.

[44] S. Takahashi, Y. Chen, and K. Tanaka-Ishii, "Modeling financial time-series with generative adversarial networks," *Physica A: Statistical Mechanics and its Applications*, vol. 527, Aug. 2019, doi: 10.1016/j.physa.2019.121261.

[45] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Systems with Applications*, vol. 143. Elsevier Ltd, Apr. 01, 2020. doi: 10.1016/j.eswa.2019.113114.

[46] B. Biswas, A. Mukhopadhyay, A. Kumar, and D. Delen, "A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks," *Decision Support Systems*, vol. 177, Feb. 2024, doi: 10.1016/j.dss.2023.114102.

[47] M. Button, “Editorial: economic and industrial espionage,” *Security Journal*, vol. 33, no. 1. Palgrave Macmillan Ltd., Mar. 01, 2020. doi: 10.1057/s41284-019-00195-5.

[48] D. Zhang, “Inconsistencies in big data,” in *Proceedings of the 12th IEEE International Conference on Cognitive Informatics and Cognitive Computing, ICCI*CC 2013*, 2013, pp. 61–67. doi: 10.1109/ICCI-CC.2013.6622226

[49] T. Y. Wu and Y. T. Wang, “Locally Interpretable One-Class Anomaly Detection for Credit Card Fraud Detection,” in *Proceedings - 2021 International Conference on Technologies and Applications of Artificial Intelligence, TAAI 2021*, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 25–30. doi: 10.1109/TAAI54685.2021.00014.

[50] G. K. Kulatilleke, “Challenges and Complexities in Machine Learning based Credit Card Fraud Detection,” Aug. 2022, [Online]. Available: http://arxiv.org/abs/2208.10943

[51] A. Kadadi, R. Agrawal, C. Nyamful, and R. Atiq, “Challenges of data integration and interoperability in big data,” in *Proceedings - 2014 IEEE International Conference on Big Data, IEEE Big Data 2014*, Institute of Electrical and Electronics Engineers Inc., 2014, pp. 38–40. doi: 10.1109/BigData.2014.7004486.