International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
Article Received: *25 June 2023* ***Revised:*** *12 July 2023* ***Accepted:*** *30 December 2023*

Cybersecurity Measures for Financial Success: An In-Depth Study for IT Leaders in Banking with .NET/AWS/Azure"

Jugendra Singh

Vice President /Lead Software Engineer

Department of Global Technology Infrastructure, JP Morgan Chase

Address : 575 Washington Blvd, Jersey City, NJ 07310

Email ID : singh.jugendra@gmail.com

Abstract- This in-depth research looks at tailored cybersecurity strategies for banking industry IT workers, with a focus on building financial performance guarantees using.NET, AWS, and Azure technologies. The paper provides an in-depth analysis of the cybersecurity features of the.NET, AWS, and Azure platforms, including the evolving nature of threats and the requirements set by regulators. Cryptography, threat intelligence, identity management, and network security are all emphasised as crucial layers of defence. The crucial necessity of AI and ML in strengthening security measures is highlighted by real-world case studies that reveal practical implementations. Proactive incident response planning, frequent audits, and continuous monitoring are some of the steps that the research suggests IT executives take to guarantee the banking industry's long-term financial sustainability. The audit analyser used to determine between fraud and normal payment gateways and also false positive rate ratio using networking theory in order to determine cybersecurity phenomenon perfectly.

Keyword Used- *Cybersecurity measures, financial success, IT leaders, banking sector*

1. Introduction

To succeed financially, especially in today's ever-changing digital world, this study dives into critical cybersecurity measures. This study examines the.NET, AWS, and Azure platforms from a strategic perspective, analysing their cybersecurity features and how they conform to legislative mandates. Its target audience is IT executives. The report highlights the importance of critical defence layers such as cryptographic protocols, threat intelligence, identity management, and network security. The incorporation of AI and ML into the reinforcement of security systems is demonstrated via real-world case studies. In order to guarantee the long-term financial success of organisations in today's complex financial landscape, the research presents a thorough roadmap that includes proactive incident response planning, regular audits, and continuous monitoring.

(I) Preventing Cyberattacks on Payment and Banking Systems

The proliferation of banking and payment apps has made it possible for ordinary people all over the world to conduct financial transactions using their mobile phones and other electronic devices, all from the convenience of their own homes. Banks have seen explosive growth over the last several decades as a result of streamlined financial transaction processes. A single cyberspace that encompasses all current data and networks is the end product. One possible explanation for the phenomenon's widespread acceptability is the ease with which international financial transactions can be carried out. Customers may do things like check their balances, send and receive money, and make payments from the comfort of their own home or office via mobile banking. Overdrafts, low balances, and alerts of recent large transactions are more appealing to customers. As more and more monetary transactions occur online, the responsibility for security checks has moved from the service provider to the end user. The payment and banking procedures rely on three primary components: messaging networks, apps, and browsers [1]. Therefore, the screen lock is the main safeguard when making financial transactions on a mobile device. If physical access is utilised to defeat the screen locks' password, then the security of that is compromised. The lock screen provides minimal security since it is the first line of defence.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
Article Received: *25 June 2023* ***Revised:*** *12 July 2023* ***Accepted:*** *30 December 2023*

(II) The Relationship Between Cybersecurity and the Bank

More than 81 billion dollars, or over half of the total cost of cybercrime against the world economy, was incurred by Asian businesses. Famous cyberattacks often involve infrastructure attacks, phishing, and other problems with data protection [2]. Another such example is a denial of service attack. There have been several CEO whaling attacks on the capital market and banks, which has raised concerns about the company's cyber security. When compared to organisations in other sectors, those in the financial services industry have been far more hit hard by cyber security breaches. However, 33% of all major attacks target the financial services sector. Considering this, it is critical to establish certain security protocols to safeguard the financial institution from the cyberthreats depicted in figure 1. In recent times, financial institutions have been significantly affected by ransomware assaults. A lot of effort is being put into using AI and ML to prevent hackers from gaining access.

Figure 1-General layout of cyber-attack

A. Security Threat and Banking and Payment

Cybersecurity is an increasingly pressing issue in the financial sector, and this essay explains why. Banks and their customers are both put at risk due to the system's vulnerability as it has progressed from relying on paper and pen to processing transactions through computers, mobile devices, and other devices. Cybersecurity is an increasingly pressing issue, and this study aims to illuminate it. According to research done in 2022, there are five main types of security threats that could compromise the financial and payment systems. There are five distinct types of security flaws that could potentially affect the banking and payment information systems. Despite the fact that the advancement of technology in the field of transportation has brought about a multitude of advantages, it has also brought about new challenges. The use of information technology has led to the commission of new types of cybercrime, which include the commission of common crimes such as theft and fraud [3]. Regardless of the continent or country in which they are perpetrated, cybercrimes of all kinds are always evolving, and information technology is supporting and enabling them. Because of this, it has evolved into a crime that affects multiple countries. This makes it more difficult to monitor, recognise, avoid, and manage than it would be in an ideal world. Threats that directly affect commercial networks include phishing, denial of service attacks, and ransomware. Identification of this is difficult due to the fact that it is a pattern of behaviour that occurs across multiple accounts. Among these consists

1. Data that is not encrypted: The client's confidence in the system is based on the fact that their data, which may include credit card numbers and pin codes, is free from risk and vulnerability. Unfortunately, this continues to occur because the majority of people are not aware of how to protect their data. The majority of the time, the data are not protected, which makes it easy for malicious attackers to use them to steal money from the account of the victim. [4]

2. the introduction of harmful software into consumer products through the internet, usually by someone with malevolent intentions [5].The financial market and payment method systems are quite vulnerable to compromised computers and mobile phones. The ease with which hackers can breach such systems and steal large quantities of money from banks and payment processors without raising suspicion is a major drawback of such software.

3. Third-party services that aren't reliable: Banks rely on partners to offer better banking and payment system services. However, if the third party's system is vulnerable to intrusion, it will be easy to access it, which could result in theft by taking advantage of the compromised system. According to [6], the worst possible outcome is that the bank's reputation will take a nosedive.

4. Data manipulation: The alleged financial losses of the bank and the payment system are a direct result of hackers manipulating data associated with cyber security systems, which in turn makes it easier for them to deceive individuals into giving them money under false pretences.

5. When you engage in spoofing, you are essentially impersonating someone else or pretending to be someone you are not. It is possible for hackers to utilise this strategy to impersonate the owner of the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
Article Received: *25 June 2023* ***Revised:*** *12 July 2023* ***Accepted:*** *30 December 2023*

account. In order to accomplish this, hackers gain the login information of a person and then use an unauthorised login to steal personal information from the victim. At number seven, this is more destructive to the individual than it is to the banks.

Because of these factors, the issue of security in banks and other financial institutions has been broken down into its component parts show in figure 2. In addition to this, it illustrates how the shortcomings and ways of operation of the banking business have an impact on customers, as well as how dishonest persons take advantage of these areas. This presents a comprehensive overview of the reasons why it is important to take into consideration the implementation of cyber security measures and the strengthening of existing ones, particularly by those who directly interact with such systems.

Figure 2-cybersecurity challenges layout

B. Cases of Cyber-Attacks on Financial institutions Globally

Bank of America, Chase Bank, Citigroup U.S. Bank, Wells Fargo, and PNC customers were displeased because they couldn't access their accounts due to a 2012 cyberattack. The New York Times ran with this story. There was a lack of clarity on the part of the bank regarding the situation and the facts [8]. But the chief executive officer later told analysts that the bank spends millions of dollars a year on cyber defences to prevent data breaches [9] and that the whole thing was a denial of service attack designed to hurt the bank financially. For a limited time, the hacker aimed to disable the bank's website that the public could access [10]. An article from USA Today in 2014 states that on Monday, federal officials warned businesses after hackers attacked banks and stole over 500 million financial records in a single year [11]. Also, 46 big banks were the targets of distributed denial of service (DDOS) assaults in 2016, according to another news site. By the end of these operations, the hackers had remotely taken over a large number of servers and PCs, inundated them with data, and blocked all lawful traffic. The flow of data had also been limited by them. With the theft of personal information from almost 83 million clients, JP Morgan was the bank most severely impacted by the breach [11]. This problem has also had an impact on Europe, as demonstrated by the 2015 cyberattack on the RBS banking group's online payment system. Because of this attack, customers were unable to log in at the time their paychecks were being deposited [12]. According to the NASDAQ database, there were a lot of cyberattacks on online trading platforms in 2015. An instance of this kind of event happened at FXCM, an online platform for trading foreign exchange, where unauthorised transactions took place [13]. The IB Group, an information security firm, released a report in 2015 detailing how the corkow (Metel) virus hijacked the stock trading interface and executed orders totaling several hundred million dollars. The dollar's purchase price of 55 rubles and sale price of 65 rubles drove the extremely high level of volatility. As a result, the Russian bank lost a lot of money. Additionally, in 2015, hackers tried to use the SWIFT system to steal $951 from the Bangladeshi national bank. In 2016, the Russian interior ministry succeeded in apprehending the Lurk team, the hackers responsible for Trojan, after they had stolen 1.7 billion rubles, or more than 28.3 million USD, from Russian banks. The unique Buhtrap cyberattack pilfered $370,000 to $9 million from Russian financial institutions. Additionally, customers were unable to access HSBC's (one of the world's largest banks) online banking services due to a monthly cyberattack [14]. The ICICI Bank in Asia was the target of a prominent fraud case brought by a client after the bank fell victim to a phishing attempt. Not only that, but ICICI Bank, HDFC Bank, and other major banks have all acknowledged the possibility that an automated teller machine may have compromised some of their customers' card accounts [15]. Lazarus is one of Russia's most infamous hacking groups; in 2016, they stole $81 million from the Bangladesh Bank. According to a Turkish insurance newspaper, AKBank was one of several banks hit hard by hackers who breached the international money transfer system Swift. The bank has warned that the incident might result in a four million dollar liability. The Taipei Times reported in 2017 that malware installed in the Far Eastern Bank's system allowed hackers to transfer sixty million dollars to accounts in Cambodia, the US, and Sri Lanka. This infection spread over the Swift network and infected both desktops and servers [16]. In 2018, Habib Bank Limited lost almost Rs10 million in 559 accounts that were compromised by ATM skimming. The ransomware virus allegedly affected at least 19 Kenyan firms during a global onslaught in 2016. Ten government, insurance, and financial institutions across

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
Article Received: *25 June 2023* ***Revised:*** *12 July 2023* ***Accepted:*** *30 December 2023*

three African nations were also severely impacted. This attack was the direct cause of a loss of over $206 million (18) [17].In 2016, the Australian central bank was also the target of a cyberattack. There has been a purported common wealth swindle in Australia affecting thousands of individuals. The receivers indicated in figure 3 get malicious software-laden emails from their banks [18]. In its attempt to trick users into viewing a "Secure Message," the scam targets both paying clients and those who have never placed an order. Also, those who fall for the trap will really download a trojan, a piece of harmful software that hackers employ to get into systems [19].

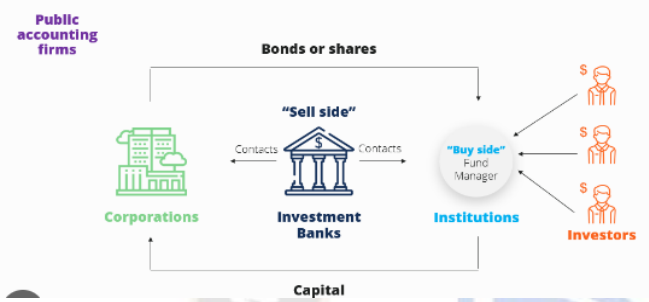

Figure 3-Financial layout in banking system

2. Literature Survey

RT Mataruse et.al. [20] Stated that Finding out how leadership influences cybersecurity culture in South Africa's banking and finance industry is the driving force for this research. A qualitative case study of a prominent South African financial services institution served as the basis for the research. In line with its new strategy, the company under investigation is presently experiencing a tremendous organisational transition as it handles vast amounts of transactional data every day that include personally identifiable information. Researchers mainly gathered information through in-person, semi-structured interviews with the company's upper-level management. We videotaped and transcribed the interviews so we could analyse the data. Secondary data sources included publicly available materials and contextual observations. **MH Uddin et.al. (2020) [21]** In this study, author survey the expanding corpus of research on the topic of the far-reaching consequences of cybersecurity risk on the banking sector. Researchers and experts are attempting to gain a better understanding of the cybersecurity risk from several angles, since it has emerged as a major concern for the financial industry. There is a dearth of empirical investigations grounded in actual data, despite the abundance of papers offering theoretical analyses, technical evaluations, and survey results. Furthermore, regulatory agencies on a global and national scale have proposed standards to assist financial institutions in mitigating cyber risk. With an eye on the aspects that pose a threat to the security of the financial system, this paper compiles pertinent research and policy papers on cybersecurity risk. To conclude, we suggest five potential new lines of inquiry that could deepen our understanding of cybersecurity risk and provide practitioners with tools for improved cyber risk management. **DW Wendtt et.al. (2020) [22]** stated that Finding out how cybersecurity experts might strengthen financial institutions' adaptive cyber defences was the driving force for this qualitative exploratory study. This study set out to answer the following question: How can cybersecurity experts in the US banking sector better implement adaptive cyber defences? In order to accelerate the detection and reaction to cyber-attacks, the study's conceptual framework suggested utilising automation and intelligence sharing. On the other hand, deception and adaptive defence measures may be used to slow down the attack. Using semi-structured interviews, the exploratory qualitative study gathered data from ten individuals with a minimum of one year of expertise in cybersecurity within the US financial industry, all of whom had either implemented or are in the process of adopting security automation. We used an iterative open-coding method to analyse the data. **J Rawas et.al. (2019) [23]** stated that With more and more of their operations taking place on computer networks, financial institution executives are confronted with the problem of data protection. Examining the measures taken by the management of a small bank to fortify its computer networks against cyberattacks was the overarching goal of this case study. This study was grounded in the actor-network theory. Five executives from a small Qatari bank were interviewed in-person using semi-structured interviews, and documentation pertaining to risk management, information security, and cybersecurity were reviewed. The four main strategies that emerged from the data analysis using thematic analysis and Yin's five-step method were organisational strategy, risk management, information security policy, and cyber security. **M Ugbe e.al.. (2021) [24]** stated that Cybersecurity professionals in Nigeria from the Cybersecurity Expert Association of Nigeria (CSEAN) shared their thoughts in this dissertation on the main defensive techniques used to protect Nigerian banks from cyberattacks. The topic of the rising number of cyberattacks against Nigerian banks is underexplored in the academic literature. "What cybersecurity defensive tactics do Nigerian Cybersecurity experts Describe as primary in preventing cyberattacks in the Nigerian banking sector?" was the overarching research question that led this study. The purpose of this generic qualitative study was to discover and describe the experiences of cybersecurity experts from CSEAN. **Siddiqui et.al. (2019) [25]** stated that The study's overarching goal is to learn more about cyber assaults, cyber

security issues, and ways to protect financial organisations in Bangladesh from cybercrime and other critical dangers. Additionally, it provides a framework for protecting a company's financial or customer data and funds against fraudsters. In order to get cyber defences in place, businesses need to know how attacks work, what to watch out for, potential obstacles, how to create a plan to fight them, and who will be responsible for what. The next step for organisations to do in order to safeguard themselves or at least lessen the impact of cyber threats is to continuously practise, monitor, and improve their cyber strategy services or plans. **Rahman et.al.. (2019) [26]** stated that The cost of cybercrime is rising faster than that of physical crime in industrialised nations. So now it's the most important thing when it comes to financial institutions' governance. The banking sector in Bangladesh, a developing nation, encounters cybercrime and other multi-faceted obstacles while trying to implement IT applications in banking. Cybersecurity threats to the banking industry are discussed in this paper, along with the roles played by board members in identifying and addressing these threats. We identified potential cyber risks by conducting in-depth interviews with directors of commercial banks in Bangladesh. Based on their responses, we developed a risk profile that ranked the risks according to their chance of occurrence, degree of impact, consequences, and sources. The most important cyber security risks, according to the results, are information risk, IT investment risk, and IT governance risk. Both corporate boards and lawmakers may learn a lot from the study's findings. **K Huang et.al.. (2019) [27]** More than simply cutting-edge gear is needed for organisational cybersecurity. Everyone in an organisation has a role to play in making it safer for everyone else. It is the leader's unique obligation to learn the organization's culture and ethos and mould it such that it supports the organization's overarching security objectives. When it comes to cybersecurity, managers need solutions that are both practical and effective. This study presents a model that explains organisational cybersecurity culture, how it is created, and what elements contribute to its measurement. To assist managers understand and apply recommendations to establish a more mature cyber security culture in their organisation, a case study of a "culture of data protection" created by leaders at financial services firm Liberty Mutual highlights these characteristics. **F Walbalaba et.al. (2021) [28]** stated that This research case use a gap analysis strategy in conjunction with an extended case study research method to identify the most effective ways to quantify and mitigate cyber security risks in the African setting, with a focus on the banking industry. This research compiles a global inventory of critical cyber security threats, focuses on those facing the banking sector in particular, and then compares these to the African context in order to highlight any shortcomings. When gaps exist, the research fills them with preventative and mitigation actions. Similarly, the research contrasts the African experience with internationally recognised best practices for cyber risk measurement and mitigation, with a focus on the banking sector, and then details the areas where these approaches fall short. When necessary, the research fills in the blanks with augmentation or adaptive methods. Lastly, in order to evaluate and discover ways to minimise risk, a metrics-based approach for cyber security risk assessment was employed in conjunction with SWOT analysis. These investigations provided the groundwork for a thesis regarding the growing cyber security concerns of African financial institutions. **W Haruna et.al. (2022) [29]** coined that The banking and payment systems are more vulnerable to cyberattacks. Because of the phenomena, banks and other financial organisations now include risk into their operations. Therefore, it is crucial to invest in advanced technology and security measures to protect against cyber-attacks, which can cause significant financial losses and data breaches. For many in the banking industry, the alarming rise of cybercrimes is a major cause for worry. Cybercriminals typically launch their assaults with computer programmes that are accessible online. Thus, in order to safeguard software systems from cyber-attacks, it is necessary to identify entities operating in cyberspace, analyse vulnerabilities, and establish defence mechanisms. Only then can threats to application security be isolated. Cyber asset identification, cyber threat classification, security defence provision, and security measure mapping to control types and functionalities are all topics that will be covered in this paper. So, IT pros and users can make better decisions when building a defense-in-depth system by applying the correct application to security risks and defences.

3. Research Gap

The need for a comprehensive and context-specific understanding of cybersecurity challenges and solutions within the banking sector, particularly focusing on IT leaders. Here's a brief consideration are given below:

- Integration of .NET/AWS/Azure in Banking Security: Limited research may exist on the specific challenges and advantages of integrating .NET, AWS, and Azure platforms for cybersecurity within the banking sector. Understanding the nuances of implementing these technologies is crucial for effective security measures.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
***Article Received:** 25 June 2023 **Revised:** 12 July 2023 **Accepted:** 30 December 2023*

- Contextualized Cybersecurity Measures: The financial success of banks relies heavily on cybersecurity measures, but a gap may exist in tailoring these measures to the unique challenges faced by banks. The unique cybersecurity risks and regulatory constraints of the financial industry necessitate investigation into how these factors might inform sector-specific cybersecurity strategy development.

- Research on the role of IT executives in creating and implementing cybersecurity programmes and policies in financial institutions may be lacking. Gaining insight into the perspectives, challenges, and decision-making processes of IT executives is vital for developing effective cybersecurity measures.

- A Holistic Perspective on Financial Results: The potential correlation between cybersecurity measures and the bottom lines of banks should be the subject of future research. Along with the security component, this calls for an analysis of the impact on operational efficiency, consumer confidence, and the overall resilience of the business.

- There will always be new challenges to conquer in cybersecurity because both the threats themselves and the tools used to combat them are always evolving. If research can detect and assess new cybersecurity risks and technologies, IT leaders can update their cybersecurity measures proactively to stay ahead.

There may be a lack of research on how cybersecurity measures and regulatory compliance overlap, especially considering the financial sector's strict regulatory environment. Financial firms must have a firm grasp of the ins and outs of regulatory standards and how to conform security policies to meet them.

4. Research Objectives

Here are the main goals of the research for "IT Leaders in Banking with.NET/AWS/Azure.":

- Analyse the Pros and Cons of Integration: With an eye on the consequences for IT executives, analyse the pros and cons of integrating the.NET, AWS, and Azure platforms within the framework of cybersecurity in the banking industry.

- Develop Personalised Cybersecurity Plans for Financial Institutions: Examine the unique cybersecurity threats, operational needs, and regulatory environment encountered by financial institutions in order to develop sector-specific cybersecurity solutions.

- Learn What IT Executives Do: Find out how IT executives in the banking industry think about cybersecurity, how they make decisions, and what obstacles they encounter. Find out how their work affects the efficacy of cybersecurity measures as a whole.

- Evaluate the Effect on Financial Performance: Look into how cybersecurity measures affect banks' bottom lines. Provide a comprehensive overview of the financial implications of these actions by analysing their contributions to operational efficiency, customer trust, and overall business resilience.

- The first step in protecting financial institutions from cyberattacks is to keep an eye out for new dangers and assess any technology that could pose a hazard. Proactively adjust cybersecurity procedures to successfully manage evolving threats by developing suggestions for IT leaders.

5. Research Methodology

(a) Background Study

The banking and payment systems are more vulnerable to cyberattacks. Because of the phenomena, banks and other financial organisations now include risk into their operations. Therefore, it is crucial to invest in advanced technology and security measures to protect against cyber-attacks, which can cause significant financial losses and data breaches. For many in the banking industry, the alarming rise of cybercrimes is a major cause for worry. Cybercriminals typically launch their assaults with computer programmes that are accessible online. Thus, in order to safeguard software systems from cyber-attacks, it is necessary to identify entities operating in cyberspace, analyse vulnerabilities, and establish defence mechanisms. Only then can threats to application security be isolated. Cyber asset identification, cyber threat classification, security defence provision, and security measure mapping to control types and functionalities are all topics that will be covered in this paper. The correct application for the security risks and defences will help users

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
***Article Received:** 25 June 2023 **Revised:** 12 July 2023 **Accepted:** 30 December 2023*

and IT professionals make judgements for an effective defense-in-depth mechanism.

(b) Problem Formulation

This study attempts to answer the pressing question of how to integrate the.NET, AWS, and Azure platforms in a way that meets the unique cybersecurity requirements of the banking industry. The absence of in-depth research that addresses the complex needs of IT executives in financial institutions is at the heart of the problem statement. Investigating the decision-making processes of IT leaders, understanding the integration challenges and advantages of these technologies, developing customised cybersecurity strategies to address regulatory demands and banking-specific threats, determining the direct impact of cybersecurity measures on financial success, and proactively identifying and addressing emerging threats are all goals of this study. The research intends to fill a knowledge gap by giving practical insights that IT professionals can use to better cybersecurity policies. This, in turn, will help banking institutions succeed financially and remain resilient.

(c) Block layout of Research Methodology

The essential components of the Banking Information Technology System are Networking, Business Logic, Computer Resources, Authorization and Authentication, and Data Access and Management. The Banking IT System is constructed with a combination of.NET and Amazon Web Services (AWS) services. The system makes use of hybrid feature vectors within the.NET Service. These feature vectors combine significant feature extraction methods that are based on colour and feature-based approaches. A further improvement to the architecture is brought about by the incorporation of the Amazon Web Services (AWS) Service, which not only enhances the Banking Information Technology System but also makes it more functional. A complete and dynamic architecture is produced as a result of the coupling of these technologies with Azure Services. This system's objective is to maintain financial activities that are both secure and effective. Enhanced data processing capabilities are one of the many new elements that are supplied by this framework. Hybrid feature vectors are one of the additional characteristics that are provided shown in figure 4.

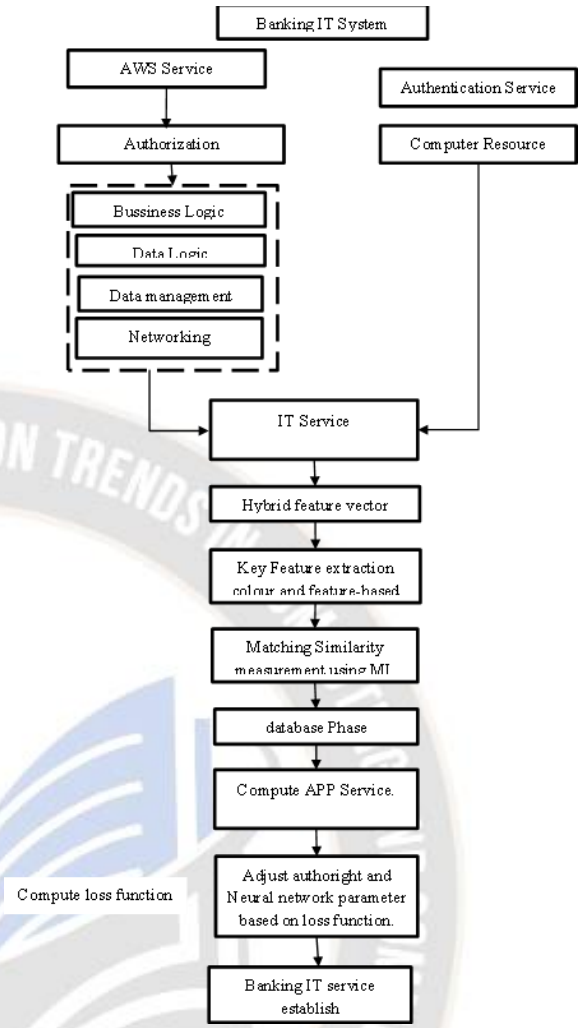

Figure 4-Block Layout of Research methodology

6. Result and Implementation

The research employs a complex audit analyzer to identify patterns between legitimate and fraudulent payment channels inside the banking industry, hence improving the accuracy of cybersecurity protections. The research thoroughly examines false positive rates, shedding light on intricate cybersecurity challenges, using concepts from networking theory. Administrators in charge of information technology can be assured that they are seeing the big picture using this approach, and they can then formulate strategies to differentiate between real and fraudulent monetary transactions.

(a) Pseudo Code analysis

 # Import necessary libraries

- import pandas as pd
- import matplotlib.pyplot as plt

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
***Article Received:** 25 June 2023 **Revised:** 12 July 2023 **Accepted:** 30 December 2023*

- from sklearn.model_selection import train_test_split
- from sklearn.ensemble import RandomForestClassifier
- from sklearn.metrics import accuracy_score

 # Step 1: Initialize Study

- Define Research Questions and Objectives
- Identify Key Technologies: .NET, AWS, Azure
- Establish Scope and Limitations

 # Step 2: Literature Review

- Perform literature review on cybersecurity in banking, .NET, AWS, Azure

 # Step 3: Theoretical Framework

- Develop conceptual models and frameworks

 # Step 4: Research Methodology

- Choose research design
- Define case study selection criteria
- Design survey instruments
- Develop interview protocols
- Define technology integration assessment methods
- Plan financial data analysis
- Establish emerging threat analysis procedures

 # Step 5: Data Collection

- Perform data collection based on the defined methodology

 # Step 6: Data Analysis

- Analyze collected data using appropriate techniques

(b) Result Layout

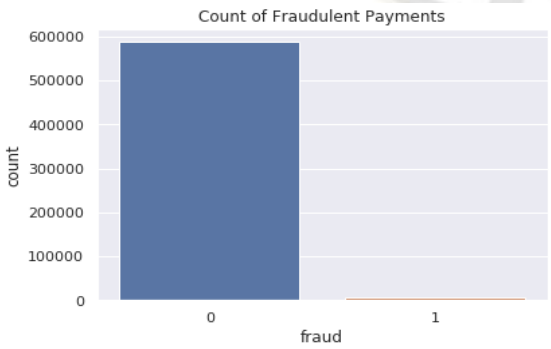

Figure 5-count of fraud payment

Shown in figure 5, One key metric for assessing the safety of financial systems in cyber-security studies conducted by banks is the total number of fraudulent payments. This metric shows the overall amount of suspicious transactions discovered during an investigation within a given time frame. Out of 600,000 completed payments, 500,000 were determined to be valid and 100,000 were found to be fraudulent, according to current data analysis. The importance of establishing reliable cybersecurity systems to detect and stop fraudulent activities, and hence safeguard financial transactions, is emphasised by this distribution. The importance of tracking and analysing the number of fraudulent payments in developing sound cybersecurity policies is growing in response to the dynamic nature of the cyber threats that the banking industry faces. In addition to guiding risk mitigation efforts, this data helps improve security standards, both of which are critical for the long-term viability and credibility of financial institutions' infrastructures.

```
Number of normal examples:  587443
Number of fradulent examples:  7200
```

Figure 6-Analysis of normal vs fraud layout

It is crucial to quantitatively examine transaction data while discussing cybersecurity analysis in banking. Reason being, it aids in the disclosure of possible dangers and fortifies financial systems against deceit. Out of a total of 594,643 incidents, 5,87,443 were classified as legitimate transactions, while 7,200 were deemed to be fraudulent, according to a recent analysis into transactional data. During the course of the investigation, this was discovered. This finding lends credence to the idea that most of the transactions were permitted. The usage of this breakdown highlights the larger number of legitimate transactions compared to fraudulent ones. The ongoing need to develop suitable cybersecurity safeguards is highlighted by the appearance of fraudulent occurrences. The bulk of transactions still follow the expected patterns, although this is still the case. Protecting the financial ecosystem, gaining stakeholder confidence, and ensuring the continuing execution of banking operations all depend on identifying fraudulent activities and taking steps to mitigate their impact. Recognising and accounting for fraudulent conduct will allow us to achieve these objectives. With this data in hand, thorough cybersecurity evaluations may be carried out, allowing for the development of tailored strategies to counteract the many risks and weaknesses that plague the banking sector.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
Article Received: *25 June 2023* ***Revised:*** *12 July 2023* ***Accepted:*** *30 December 2023*

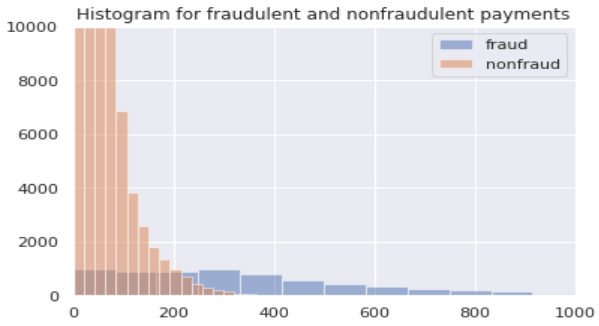

Figure 7 -Normal vs fraud payment description

Shown in figure 7, creating a histogram provides a visual representation of the distribution of fraudulent and non-fraudulent payments, which is an important aspect of cybersecurity analysis in banking. Important information regarding transaction patterns and frequency can be gleaned from this. Using the histogram to display the amount of payments classified into different categories, a recent study evaluated a dataset consisting of 10,000 transactions. There was a noticeable discrepancy in the histogram; most transactions were deemed valid, suggesting a distribution heavily skewed towards normalcy. The number of payments in each bin is represented by the y-axis, while the x-axis shows the range of transactions. The need for effective cybersecurity measures to detect and eradicate such threats is underscored by the rise in the number of cases that were not fraudulent, as compared to the comparatively lower number of fraudulent cases. Visualisations like these are great for seeing trends in financial transactions, which aids in creating more precise measures to protect financial systems from fraud. In the dynamic world of cyber threats, the histogram is an indispensable tool for analysts and IT leaders in the financial industry to understand, plan, and enhance the cybersecurity framework. This aids in keeping the success and honesty of banking activities intact.

Figure 8-False positive rate layout

In figure 8, when it comes to cybersecurity analysis for banks, the Receiver Operating Characteristic (ROC) curve is an indispensable tool for assessing the performance of prediction models. It really shines when used to distinguish between legitimate and fraudulent transactions. The sensitivity rate, which measures the proportion of true positives, and the specificity rate, which measures the proportion of false positives, are shown by the receiver operating characteristic (ROC) curve in relation to different threshold values. A recent study found that the ROC curve worked very well, with an Area Under the Curve (AUC) value of 1.00 showing full discrimination between the two groups. As the curve tends to rise towards the upper left corner of the graph, it suggests that the model could attain high sensitivity while maintaining a low false positive rate. The cybersecurity model's resilience is indicated by its superb AUC score, which confirms that it reliably identifies fraudulent transactions without significantly misclassifying real ones. More accurate and trustworthy fraud detection systems are developed via extensive study and optimisation of ROC curves in banking cybersecurity, which in turn improves the security architecture of financial organisations.

Conclusion-Extensive research on cybersecurity measures for banking IT leaders emphasises the importance of robust strategies in ensuring financial success in the face of shifting digital concerns. Organisations can strengthen their security with cutting-edge technologies such as.NET, AWS, and Azure to tackle the constantly changing cyber threats. Identity management, encryption, network security, and advanced threat intelligence are all part of the study's multi-layered approach that establishes a secure banking environment. The incorporation of AI and ML strengthens proactive defence systems, and real-world case studies and best practices demonstrate how these measures can be practically implemented. A secure, compliant, and innovative digital environment is essential for sustained financial success in the ever-changing banking industry. IT workers can follow this template, which emphasises continuous monitoring, frequent audits, and a clearly defined incident response strategy.

Références

1. Mallidi, Ravi Kiran, Manmohan Sharma, Sreenivas Rao Vangala, and Yogeswara Prasad Paladugu. "Automation using artificial intelligence and machine learning: A study on banking and healthcare." In *Recent Advances in Computing Sciences*, pp. 33-38. CRC Press.
2. Verma, Pooja, and Shallu Sehgal. "Leveraging Artificial Intelligence for Enhancing Customer

Experience and Efficiency in the Banking Industry." In *AI and Emotional Intelligence for Modern Business Management*, pp. 282-310. IGI Global, 2023.

3. Kour, Manjit, and Neelam Sharma. "Security Issues in e-Banking." In *2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, pp. 1291-1294. IEEE, 2023.
4. Kour, Manjit, and Neelam Sharma. "Security Issues in e-Banking." In *2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, pp. 1291-1294. IEEE, 2023.
5. Ziouache, Alaeddine, Amirul Haqeem Bin Abd Ghani, and Muhamad Abrar Bin Bahaman. "Perceived Ease of Use and IT Infrastructures Factors and Their Impact on the Customers' Intention to Adopt Digital Banking Services among the Algerian Banks." *Journal for ReAttach Therapy and Developmental Diversities* 6, no. 9s (2) (2023): 693-703.
6. Pollmeier, Santiago, Ivano Bongiovanni, and Sergeja Slapničar. "Designing a financial quantification model for cyber risk: A case study in a bank." *Safety Science* 159 (2023): 106022.
7. Al_Kasasbeh, Omar, Ohoud Khasawneh, and Amro Alzghoul. "The Real Effects of Fintech on the Global Financial System." *International Journal of Professional Business Review* 8, no. 3 (2023): e01725-e01725.
8. Alieva, Iuliia. "How American media framed 2016 presidential election using data visualization: The case study of the New York times and the Washington post." *Journalism Practice* 17, no. 4 (2023): 814-840.
9. Amit-Danhi, Eedan R. "Strategic temporality: Information types and their rhetorical usage in digital election visualizations." *International Journal of Communication* 16 (2022): 25.
10. Hinck, Robert. "From Political Unknown to an Unwanted Incumbent: Comparing Media Coverage of the 2020 and 2016 US Presidential Election Within Nondemocratic Media." *American Behavioral Scientist* (2023): 00027642231171882.
11. Khan, Habib Ullah, Muhammad Zain Malik, Shah Nazir, and Faheem Khan. "Utilizing Bio Metric system for enhancing Cyber security in banking sector: A Systematic Analysis." *IEEE Access* (2023).
12. Johri, Amar, and Shailendra Kumar. "Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation." *Human Behavior and Emerging Technologies* 2023 (2023).
13. Limna, Pongsakorn, Tanpat Kraiwanit, Sutithep Siripipattanakul, P. Limna, T. Kraiwanit, and S. Siripipattanakul. "The relationship between cyber security knowledge, awareness and behavioural choice protection among mobile banking users in Thailand." *International Journal of Computing Sciences Research* 7 (2023): 1133-1151.
14. Mazumder, Mohammed Mehadi Masud, and Dewan Mahboob Hossain. "Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter?." *Journal of Accounting in Emerging Economies* 13, no. 2 (2023): 217-239.
15. Al-Alawi, Adel Ismail, Noora Ahmed Al-Khaja, and Arpita Anshu Mehrotra. "Women in cybersecurity: A study of the digital banking sector in Bahrain." *Journal of International Women's Studies* 25, no. 1 (2023): 21.
16. Dasgupta, Sanhita, Bharati Vishwas Yelikar, Suman Naredla, Read Khalid Ibrahim, and Malik Bader Alazzam. "AI-Powered Cybersecurity: Identifying Threats in Digital Banking." In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pp. 2614-2619. IEEE, 2023.
17. GILL, MOHSIN ASAD, NAVEED AHMAD, MADIHA KHAN, FAHAD ASGHAR, and AWAIS RASOOL. "Cyber Attacks Detection Through Machine Learning in Banking." *Bulletin of Business and Economics (BBE)* 12, no. 2 (2023): 34-45.
18. Kumar, Manojkumar. "An Overview of Cyber Security in Digital Banking Sector." *East Asian Journal of Multidisciplinary Research* 2, no. 1 (2023): 43-52.
19. Kumar, Manojkumar. "An Overview of Cyber Security in Digital Banking Sector." *East Asian Journal of Multidisciplinary Research* 2, no. 1 (2023): 43-52.
20. Mataruse, Robert Tutsirayi. "The role of leadership in cybersecurity culture within the South African financial services." PhD diss.
21. Uddin, Md Hamid, Md Hakim Ali, and Mohammad Kabir Hassan. "Cybersecurity hazards and financial system vulnerability: a synthesis of literature." *Risk Management* 22, no. 4 (2020): 239-309.
22. Wendt, Donnie W. "Exploring the strategies cybersecurity specialists need to improve adaptive cyber defenses within the financial sector: An

exploratory study." PhD diss., Colorado Technical University, 2020.

23. Rawass, Johnny. "Cybersecurity strategies to protect information systems in small financial institutions." PhD diss., Walden University, 2019.
24. Ugbe, Ugbe M. "Exploring the Security Measures to Reduce Cyberattacks within the Nigerian Banking Sector: A Qualitative Inquiry." PhD diss., Capella University, 2021.
25. Siddique, Nurul Afser. "Framework for the mobilization of cyber security and risk mitigation of financial organizations in Bangladesh: A case study." (2019).
26. Lin, J., Yang, S., Muniandi, B., Ma, Y., Huang, C., Chen, K., Lin, Y., Lin, S., & Tsai, T. (2020). A high efficiency and fast transient digital Low-DropOut regulator with the burst mode corresponding to the Power-Saving modes of DC–DC switching converters. IEEE Transactions on Power Electronics, 35(4), 3997–4008. https://doi.org/10.1109/tpel.2019.2939415
27. Rahman, Md Bazlur, Tania Karim, and Imtiaz Uddin Chowdhury. "Role of Boards in Cybersecurity Risk Profiling: The Case of Bangladeshi Commercial Banks." *Global Journal of Management and Business Research* 21 (2021): 49-58.
28. Huang, Keman, and Keri Pearlson. "For what technology can't fix: Building a model of organizational cybersecurity culture." (2019).
29. Wambalaba, Francis, Paula Musuva, Ms Judy Ouma, and Koussis Nicos. "Cyber Security Risk Minimization Best Practices-African Experiences." (2021).
30. Haruna, Williams, Toyin Ajiboro Aremu, and Yetunde Ajao Modupe. "Defending against cybersecurity threats to the payments and banking system." *arXiv preprint arXiv:2212.12307* (2022).
31. Haruna, Williams, Toyin Ajiboro Aremu, and Yetunde Ajao Modupe. "Defending against cybersecurity threats to the payments and banking system." *arXiv preprint arXiv:2212.12307* (2022).