Journal of Excellence in Social Sciences (2024) 3(3):191–210
ISSN (E): 2755-3876

The Impact of Cybercrime Incidents and Artificial Intelligence adoption on Organizational Performance: A Mediation and moderation model

Munaza Bukhari[1]

Shahzadi Sattar[2]

Sajjad Saleem*[3]

Khan Zaman Khan[4]

Ansa Khan[5]

How to cite this article:

Bukhari, M., Sattar, S., Saleem, S., Khan, K. Z., & Khan, A. (2024). The impact of cybercrime incidents and artificial intelligence adoption on organizational performance: A mediation and moderation model. *Journal of Excellence in Social Sciences*, *3*(3), 191–210.

Received: 8 June 2024 / Accepted: 27 July 2024 / Published online: 29 August 2024

Abstract

Financial fraud, intellectual property theft, and domains undergo high threats due to cybercrime, increasing the threat to businesses, especially financial markets. Such dirty activities hit various organizations, whether banks, financial institutions, corporations, or individuals, and jeopardize those activities that depend on financial support. Technology has brought many changes with its integration into the financial sector. Although technology has made it easier to handle business tasks day in and day out, the ease of using technology has also given rise to cyberattacks. The arrival of artificial intelligence has brought in new models to combat these cyber threats and also assess them. People must become smart about AI so that they don't get duped. This research aims to expand upon the fraud diamond framework by identifying risk factors leading organisations toward fraudulent behaviour. It focuses on the relationship between artificial intelligence, cybercrime incidents and organizational performance. It is proposed that fraud cases can act as mediators, while cyber threats may serve as moderators, impacting organizational performance. Descriptive research, useful for unbiased data collection that accurately reflects behaviour and trends, was applied. Data was collected from bank managers, operations managers, assistant vice presidents, and executive leaders through a convenience sampling method, a non-probability approach. 550 questionnaires were

[1]National College of Business Administration & Economics, Lahore (Multan Campus), Punjab, Pakistan
[2]National Fertilizer Corporation Institute of Engineering and Technology Multan, Pakistan.
[3]Washington University of Science and Technology, Virginia, United States.
Corresponding Author: ssaleem.student@wust.edu
[4]Noon Business School, University of Sargodha, Punjab, Pakistan.
[5]School of Business Management, University Utara Malaysia, Kedah, Malaysia.

distributed via Google Forms, yielding an adequate response rate. Partial Least Squares Structural Equation Modeling (PLS-SEM) software was used for data analysis. The findings underscore the need for international cooperation among governments, regulators, law enforcement, and financial institutions to address the global nature of cyber threats. Such cooperation is crucial for effectively managing, responding to, and mitigating the risks posed by these incidents.

Keywords: Cyber Crime Incidents, Artificial Intelligence adoption, Organizational Performance, Fraudulent Cases, Cyber threats, Banks.

1 Introduction

Cybercrime, unlike traditional offences, affects multiple jurisdictions and influences society in various ways (Graham, 2023). It refers to any crime executed with or heavily dependent on computing elements, such as computers or mobile phones (Goni et al., 2022). These electronic devices serve as facilitators and agents of crime (Blythe & Johnson, 2021). Cybercriminals exploit the obscurity, privacy, and interconnectivity of the internet to attack and undermine the very backbone of our modern information society. Banks and financial institutions, mainly, are highly concerned about breaches in their cyberspace (Uddin et al., 2020). With large economic stakes, the threat of data theft continues to grow, making banks a prime target for cyber-attackers due to the valuable customer information they store.

Additionally, it is argued that banks are prime targets for hackers due to their expertise in accessing financial systems. Electronic financial services, including ATMs, mobile banking, and Internet banking, are at risk of fraud attacks like skimming and phishing (Uddin et al., 2020). For affected banks, there is also the risk of a drop in share prices. The banking industry is especially vulnerable to cybersecurity breaches because of the high financial gains for attackers (Ghelani et al., 2022). In Pakistan, the banking sector is rapidly expanding, so overall threats are also on the rise (Riaz et al., 2024). Financial services such as account details and credit card information are at risk of theft or falsification (Beju & Făt, 2023). The country has faced significant cyber breaches in the banking sector, including a 2018 incident where inadequate online security allowed foreign hackers to steal customer data, resulting in a $6 million loss. That same year, a PakCERT analysis revealed that data from 19,864 debit cards from 22 Pakistani banks was listed for sale on the dark web (Bukht et al., 2020; Khattak et al., 2021).

Additionally, cyber breaches on January 24 and January 30, 2019, exposed significant data from Meezan Bank Ltd. Gemini Advisory, a cybersecurity group addressing cyber threats, linked these records to a breach in Meezan Bank Limited's internal systems (Firdaus et al., 2022). Fraudsters leverage fake cards, often using "money mules" to withdraw cash from ATMs or buy resold goods (Shetty & Murthy, 2023). On February 22, 2019, cybersecurity firm Group-IB highlighted that despite banks' efforts to curb ATM fraud, criminals continue to bypass security and retrieve card data at points of sale (Shulzhenko & Romashkin, 2020). A single cyber-attack can result in major financial losses, intellectual property theft, and erode consumer confidence (Kao, 2020). Cybercrime costs society and governments billions annually. Although Pakistani banks claim insurance policies (Saleem et al., 2024), many show limited interest in securing their systems, exposing the public to cyber-attacks (Bukht et al., 2020). The distrust in online banking grows, and inadequate insurance coverage leads many to prefer storing their money at home. This trend has contributed to a decline in the country's economy.

Pakistan must bolster its cyber infrastructure while investing in its youth to help develop a workforce of cybersecurity specialists (Arshad et al., 2024). This includes designing cybersecurity, ethical hacking, and information security courses to build a generation of young professionals prepared to address new cybersecurity challenges (Nicholson et al., 2021). Intensify efforts to leverage emerging technologies — AI, blockchain, robotic process automation — to improve

cybersecurity (Khan et al., 2024). This suggests a robust cyberinfrastructure annex specifically for the IT-enabled services sector, especially for the banking sector, which may drive economic prosperity and stability by attracting FDI and fostering innovation (Huan & Qamruzzaman, 2022). Moreover, international borders do not restrict cybercrime, so Pakistan must collectively work with other states and form partnerships to share resources and best practices (Akram et al., 2023). Establishing an overall legal and policy framework is also important, including passing laws that address cybercrime and developing policies that advance cybersecurity and protect citizens' rights (Haider et al., 2024). Pakistan can strengthen its cybersecurity landscape, a significant building block for security and resilience (Haque et al., 2023), considering the cyber threats that the world is facing (Muhammad et al., 2022; Tahir et al., 2019).

Pakistan Cyber Law dwells on international cooperation as the central theme. Pakistan is a member of the International Multilateral Partnership against Cyber Threats (ITU-IMPACT) and the APSIRC-WG (Asia Pacific Security Incident Response Coordination Working Group) (Khan et al., 2021). Nonetheless, these initiatives have not yielded significant attention to cybersecurity within the country's international conversation and agreements. Pakistan should collaboratively identify deficiencies regarding the context of the matter, which is significant in reviewing the Prevention of Electronic Crimes Bill (Sultan & Mohamed, 2023), as it plays a vital role in improving the security of banking systems. Cybercrime, cyber-attacks, and cybercrime-related fraud incidences have been causing lower organizational performance and major challenges for the Pakistani banking sector (Gilani et al., 2023). A more robust legal framework will strengthen the resilience of these financial institutions and the confidence of consumers and investors, and in turn, a safer and more stable banking landscape. To even begin tackling this continuous whack-a-mole of threats and as a stepping stone toward global cybersecurity, Pakistan needs to make cybersecurity visible on the international cooperation agenda (Khalil, 2020).

2 Literature Review

2.1 Cyber Crime Incidents, Fraudulent cases, and Organizational performance

In this study, fraud is operationalized as deception, where one party deliberately misrepresents itself to trick another, often called the victim. In the world of e-commerce (Chen et al., 2024), this can manifest as misleading information resulting from illegal or one-sided online business practices, which we might call an illegal error. The growing popularity of e-commerce has opened up many new payment options and accessories (Beyari, 2021). However, it has also led to a rise in innovative ways for fraudsters to exploit the internet. With the rapid increase in online connections, there is a greater risk of theft and significant financial losses (Monteith et al., 2021; Nicholls et al., 2021). This surge in fraudulent activity has also become a major challenge for e-commerce (Alqethami et al., 2021; Rodrigues et al., 2022). While various strategies are being implemented to combat online fraud, it is also essential to consider the specific vulnerabilities in the Gulf region (Cavaliere et al., 2021).

Organized crime groups increasingly leverage the Internet to commit significant fraud and theft (Ibrahim, 2022). Trends show a clear connection between these groups and white-collar crime as they shift away from traditional methods to take advantage of online opportunities (Gottschalk & Hamerton, 2021). Internet-based stock fraud, in particular, has become a lucrative avenue for criminals, netting them millions yearly and resulting in substantial investor losses (Clinton, 2023). Police departments nationwide have reported a growing number of these crimes in recent years. This rise aligns with a national trend linked to the increasing use of computers, the growth of online business, and the emergence of highly sophisticated cyber criminals (Wall, 2024). Notably, in 2004, cybercrime generated more profit than drug trafficking, and as technology continues to expand, especially in developing countries, this trend is expected to grow even further (Saini et al., 2012). The root causes of cybercrime are apparent when we look closely at society (Pasculli, 2020). One can easily notice the display of ill-gotten wealth and how many perpetrators are

celebrated or admired. This issue is exacerbated by high youth unemployment rates, a lack of enforceable laws against cybercrime, and a general indifference among individuals and businesses toward cybersecurity (Hassan et al., 2012). Research indicates that many of these crimes are committed by young people. However, it is important to recognize that many cyberattacks occur within organizations (Ullah et al., 2021; Yeboah-Ofori & Opoku-Boateng, 2023). Many internet users fall prey to scams, easily lured by suspicious emails and questionable website links, which can lead to spyware infections and phishing attacks.

Hassan et al. (2012) identified several key factors contributing to the rise of cybercrime, including urbanization, high unemployment rates, the pursuit of wealth, ineffective enforcement of cybercrime laws, poorly equipped law enforcement agencies, and the influence of negative role models. In a separate report by Akwara et al. (2013), the researchers stated that unemployment tends to generate poverty, which has a positive causal relationship with insecurity. They also identified other drivers of cybercrime, like corruption, human naivety and greed, the presence of cyber cafes, and the inherently vulnerable nature of the internet, which acts as a "superhighway" waiting for explorers.

Cybercrime takes a toll on an organization's productivity; businesses spend time and resources to keep their networks secure from attacks (Ene & Imo, 2024; Yeboah-Ofori & Opoku-Boateng, 2023). In-house cybersecurity is essential, beginning with round-the-clock monitoring (Alghamdi & Schukat, 2020). However, it consumes time, which can be used for core operations, thereby successfully reducing overall productivity. The three components mentioned above will enable corporations to purchase software with security to combat viruses and other malware (Javaid et al., 2023), forcing them to eat the burdensome overhead to the detriment of profit margins (Arenas et al., 2024). The cost of cybercrime comes not only from the economic cost itself (Franjić, 2020), but also from the indirect cost of computers and network resources being under stress and from lost opportunity costs when dealing with impersonal messages. These costs burden the wider economy and business, usually encompassing the loss of intellectual property, financial fraud, reputation damage, productivity costs, and third-party liability (Iftikhar, 2024). For example, lost sales and reduced productivity are other examples of the total costs reported by cyberattacks and viruses (Bhakhri et al., 2023; Kokaji & Goto, 2022). But, as exciting as these opportunity costs appear, opportunity costs do not always imply larger economic deficits. Cybercrime poses a considerable threat to enterprises, especially finance-related businesses, where financial fraud and intellectual property theft are major concerns. According to 2016 research by the Ponemon Institute, the annual cost of cybercrime in six countries — the USA, Japan, Germany, the UK, Brazil, and Australia — ranged from $4.3 million to $17.3 million (Mostafa, 2022; Onwunyi & Okonkwo, 2021). A healthy economy depends on an open and functioning financial system, and many cyberattacks are financially motivated. Consequently, these criminal activities impact banks, financial institutions, enterprises, and individuals, affecting the financial stability of organizations that rely on them.

Therefore, the following hypotheses can be deduced from the following literature:

H1: *Cybercrime incidents significantly affect fraudulent cases*

H2: *Cybercrime incidents significantly affect organizational performance with the mediating effect of fraudulent cases*

2.2 Artificial intelligence adoption, fraudulent cases, and organizational performance

A growing focus has recently been on developing artificial intelligence (AI) to detect fraudulent banking operations (Alhaddad, 2018; Bello & Olufemi, 2024). The focus on preventing fraud has intensified due to the growing incidence of fraud in the banking sector, causing substantial financial losses for banks and customers (Gautam, 2023). AI-based systems offer real-time recognition and prevention of fraud, providing a significant advantage over traditional fraud

detection methods (Hassan et al., 2023). AI and machine learning algorithms assist analysts in examining large datasets from various sources (Sarker, 2021), such as transaction logs, user profiles, and network logs, to identify suspicious banking activities (Ketenci et al., 2021). These algorithms can detect patterns and anomalies that may indicate fraudulent actions, such as unauthorized access, abnormal transaction patterns, and suspicious activities (Gayam, 2020; Hilal et al., 2022). A bank transaction refers to any bank account activity occurring online or offline among all parties. The transaction is completed once a written or electronic payment order is submitted to the bank through Internet banking, communication channels, or specific payment methods (Jansen & Leukfeldt, 2015).

Fraud is constantly evolving, which means we need to do the same. Here are five ways bank fraud can be prevented: Artificial Intelligence (AI) (King et al., 2020), which leverages huge datasets held by financial service providers to sift through extensive transaction data in real-time to detect suspicious activity (Sohel et al., 2024); biometric methods like fingerprint or facial recognition, providing an extra layer of security that is challenging even for advanced fraudsters (Arora & Bhatia, 2022; Kumar et al., 2024); consortium data, which enables banks and financial institutions to share data for insights on fraud trends—insights that may not be visible to a single institution alone (Javaid, 2024). Additionally, standardized security protocols across the industry could strengthen defences against fraud schemes, while machine learning, constantly evolving from new data, enhances anomaly detection and reduces false positives over time. Applications in fraud detection, with their potential for high efficiency and accuracy, represent a vibrant research area. Yet, alongside these advantages, challenges and concerns about using AI in banking must be addressed to ensure its effectiveness and ethical application (SailPoint, 2021).

AI applications for detecting fraud in banking activities are an area of active research with great potential for enhancing fraud detection efficiency (Bello & Olufemi, 2024). However, to ensure its effectiveness and ethical use in the banking sector, address the challenges and concerns associated with implementing AI in this context (Mytnyk et al., 2023). While technology advances, fraudsters leverage it to develop increasingly sophisticated schemes. These actions can lead to substantial financial losses, damage to an organization's reputation, and a loss of public trust. Organizations are adopting advanced technological tools to counter these growing risks and strengthen their fraud detection capabilities. These tools are designed to handle complex tasks, such as problem-solving, decision-making, and identifying patterns, that were once possible only through human expertise (Mohammed & Rahman, 2024).

Therefore, the following hypotheses can be withdrawn:

H3: *Artificial intelligence adoption significantly affects the fraudulent cases*

H4: *Artificial intelligence adoption significantly affects organizational performance with the mediating role of fraudulent cases*

2.3 Cybercrime incidents, Artificial intelligence, fraudulent cases, cyber threats and organizational performance

2.3.1 Fraud Diamond Theory

To better understand cyber threats, it's essential to recognize their motivations. One key theory explored in this study is the "Fraud Diamond Theory," which expands on the well-known "Fraud Triangle" model (Arkorful et al., 2022). Originally developed in 1953 by criminologist Donald Cressey, the Fraud Triangle model seeks to explain why individuals commit fraud (Tickner & Button, 2021). Cressey's research focused on those he termed trust violators, particularly embezzlers. According to the theory, three core components must be present for fraud to occur: a perceived, non-shareable financial need (incentive), a perceived opportunity, and a rationalization for the behaviour (Kagias et al., 2022).

Research indicates that financial pressure on an individual increases the likelihood of fraud, opportunities (due to weak controls or lack of monitoring), and a rationalization process that the scam is justified (Dorminey, 2012; Wolfe & Hermanson, 2004). These three tools run together to help outline the possibility of fraud and its significance. A "trust violator" is someone Cressey describes as someone put into a position of trust and encounters a perceived, non-shareable financial problem (Klenowski & Copes, 2020). But this one issue doesn't drive people to commit sins. The fraud triangle tells us all three must be present for a breach of trust — financial pressure, opportunity, and rationalization (Kagias et al., 2022). Perceived opportunity is the second element, and it relates to the opportunities for committing a crime, often due to weak controls or little supervision that leads a person not to perceive committing fraud as a desirable act. The third element, rationalization, is essential for excusing dishonest behaviour (Aksa et al., 2020). People rationalize their actions, often seeing themselves not as criminals but as unfortunate victims of circumstance. According to Cressey's theory, an embezzler must internally justify the act to perceive it as a justifiable cause rather than a crime (Vousinas, 2018).

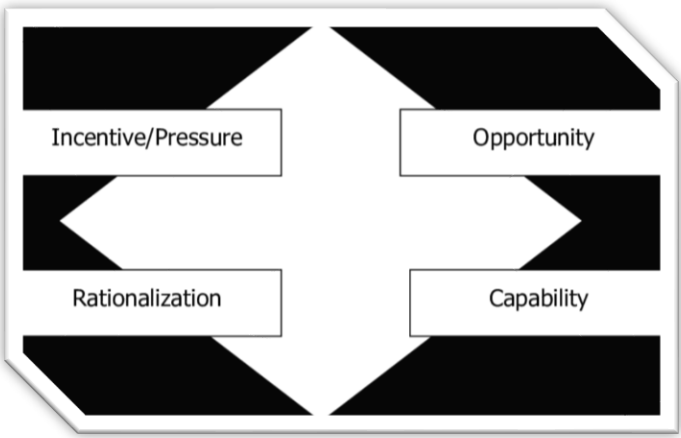

Figure 1: Fraud Diamond Model

Wolfe and Hermanson (2004) proposed that adding a fourth component to the fraud triangle could enhance fraud detection. Known as the "fraud diamond" theory, the authors first introduced this model in December 2004. The four sides of the fraud diamond—pressure, opportunity, rationalization, and capability—each play a key role, with capability determining whether fraud will occur, even if the other three conditions are present. Many major frauds, especially high-value ones, would not have occurred without the involvement of a person with the necessary capabilities. Capability refers to the skills or knowledge required to carry out the fraud. Wolfe and Hermanson emphasized that pressure, opportunity, rationalization, and capability must all be present for an offence to occur.

Recognizing the relevance of the fraud diamond theory to the financial sector enables individuals and organizations to identify and prevent potential fraud. This awareness, combined with fostering an ethical culture, may also require stronger financial controls and compliance measures. According to Firdaus et al. (2022) the fraud diamond theory has effective potential in managing cyber threats in the presence of AI capabilities. According to Wiafe et al. (2020), cyber threats are not limited to attacks conducted by individuals or groups but instead, any criminal act that relies on the use of a communication device or information system and thus manifests itself in electronic or cyber form for the purpose of intimidation, harm, or damage. This may include everything from viruses and malware to phishing and ransomware attacks targeting computer networks, systems, and devices to perpetrate fraud, steal data, incapacitate systems, and disrupt operations and

services (Al-Khater et al., 2020).

In the financial sector, cyber threats have become increasingly dire, with the increase in fraud cases only showing how clever fraudsters are becoming in leveraging digital technologies. They employ techniques such as phishing, identity theft, and online fraud to steal personal or financial information. Their targets vary from people and companies to government organizations, as do their attacks — which can unfold online or in person. The article emphasizes that by applying AI and ML to the four pillars of fraud diamond theory, which are rationalization, motivation, opportunity, and capability, organizations will be in a strong position to both detect, predict and effectively respond to these kinds of cyber fraud, thereby resulting in a more robust defence against the ever-evolving nature of online fraud. While negligence and money laundering are important contributors to the rising trend of fraud in the financial industry, systemic weaknesses are also essential enablers that empower fraud. While nothing new, cyber threats have become so advanced that traditional defenses are often ineffective. It is a classic example of why we need a balance of humans and machines to fight cybercrime. From the above literature, the following hypotheses can be drawn:

H5: *Cybercrime incidents affect organizational performance through fraudulent cases, so the indirect effect will be weaker at different levels of Cyber threats.*

H6: *Artificial intelligence adoption affects organizational performance through fraudulent cases, so the indirect effect will be weaker at different levels of Cyber threats.*

2.4 Conceptual Framework

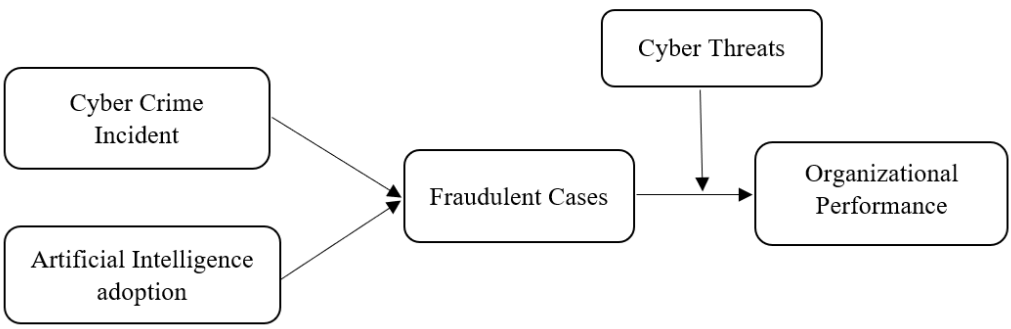

Figure 2: Conceptual Framework

3 Methodology

3.1 Research Design

This study used quantitative research to quantify variables and derive meaningful results. The selected research design was descriptive research, which is theory-based and relies on systematically collecting, evaluating, and presenting data. Descriptive research is particularly effective for gathering unbiased information that reflects behaviours or recurring events (Romanchuk, 2024). This study used a convenience sampling method, a non-probability sampling technique where subjects are selected from the population because of their convenient accessibility and proximity to the researcher. This choice can depend on geographical proximity and when the subjects were available or willing to participate. Also known as convenience sampling, this is a type of non-probability sampling (Nikolopoulou, 2022).

Convenience sampling offers researchers a practical way to gather data quickly by engaging participants who are easy to reach. Primary data, original, unpublished information obtained

directly from respondents, was collected for this study (Crowther, 2012). The main data collection tool was a questionnaire, chosen for its effectiveness in efficiently gathering quantitative data from a large sample. This approach offers advantages such as a streamlined data collection process, allowing researchers to acquire insights quickly and accurately.

3.2 Sample size

The population selected for the data collection constituted of Scheduled banks, i-e, Public Sector Commercial Banks (First Women Bank Ltd., National Bank of Pakistan, Sindh Bank Ltd., The Bank of Khyber, The Bank of Punjab), Specialized banks (Industrial Development Bank of Pakistan. SME Bank Ltd., The Punjab Provincial Cooperative Bank Ltd., Zarai Taraqiati Bank Ltd) Domestic Private Banks (Al Baraka Bank (Pakistan) Ltd., Allied Bank Ltd., Askari Bank Ltd., Bank Al Falah Ltd., Bank Al Habib Ltd., Bank Islami Pakistan Ltd., Dubai Islami Bank Pakistan Ltd., Faysal Bank Ltd., Habib Bank Ltd., Habib Metropolitan Bank Ltd., JS Bank Ltd., MCB Bank Ltd., MCB Islamic Bank Ltd., Meezan Bank Ltd, Samba Bank Ltd., Silk bank Ltd., Soneri Bank Ltd., Standard Chartered Bank (Pakistan) Ltd., Summit Bank Ltd., United Bank Ltd.), Microfinance Banks (Finca Microfinance Bank Ltd. ,U Microfinance Bank Ltd., Khushhali Bank Ltd., Advance Pakistan Microfinance Bank Ltd., Sindh Microfinance Bank Ltd., NRSP Microfinance Bank Ltd., Telenor Microfinance Bank Ltd., Pak Oman Microfinance Bank Ltd., Apna Microfinance Bank (formerly Network Microfinance), The First Microfinance Bank Ltd., Mobilink Microfinance Bank Ltd). The target respondents were bank managers, operation managers, AVPs, and presidents, who occupy managerial positions either way.550 questionnaires were distributed among upper-echelon positions through Google Forms, and they were smartly filled out and submitted.

3.3 Measures

Organizational Performance: To assess organizational performance in financial institutions where OP was measured based on scales developed by Kafetzopoulos and Psomas (2015). The respondents assessed their organization's performance relative to similar entities.

Cybercrime Incidents: Respondents reported the frequency of various cybercrime types their organization encountered over the past year, with response options ranging from "never" to hundreds of times daily. These questions were based on the framework from Paoli et al. (2017) and were mandatory for all businesses.

Fraudulent Cases: Adapted from Kazemian et al. (2019) and Rahman et al. (2021), this section focused on fraud risk factors, particularly asset misappropriation in banking, and the integration of artificial intelligence (AI) in fraud detection and prevention.

Artificial Intelligence Factors: Drawing on Xia et al. (2022) and Rahman et al. (2021), this section examined three AI dimensions: Autonomy (individual choice in learning AI), Competence (facilitation of AI learning), and Relatedness (interpersonal involvement in AI-related activities).

Cyber Crime Threats: Questions adapted from Kazemian et al. (2019) and Salameh and Lutfi (2021) explored cybercrime risks, especially in banking, and assessed the influence of AI in mitigating these threats. This comprehensive survey design enabled the researchers to gather detailed data on cybercrime incidence, fraud risks, and AI-driven mitigation strategies within organizations.

4 Data Analysis

Data was analyzed using partial least squares-structural equation modelling (PLS-SEM), as Bido et al. (2014) recommended. SmartPLS 4 was selected as it is a reliable second-generation analysis tool that employs a variance-based approach (Hair et al., 2017). This software simultaneously evaluates all model interactions (Hair et al., 2017; Kock & Hadaya, 2018). Given the study's

predictive objective toward endogenous variables, PLS-SEM was deemed most suitable (Hair et al., 2017). Although PLS-SEM does not assume data normality, data distribution was visually checked, revealing a normal distribution via histograms and normal probability plots in SPSS 27 (Pallant, 2010). Since all constructs in this research are reflective and first-order, PLS-SEM was an appropriate choice. Hair et al. (2017) suggest assessing the measurement model before the structural model, requiring reliability and validity evaluations for each reflective construct. To test internal consistency and convergent validity, the outer loadings of items in each construct ranged from 0.770 to 0.863 (Duarte & Raposo, 2010; Hair et al., 2017). Figure II illustrates the measurement model. Composite reliability (CR) values ranged from 0.812 to 0.941, while Cronbach's alpha values from 0.793 to 0.936 confirmed satisfactory internal consistency (Bagozzi & Yi, 1988; Hair et al., 2017).

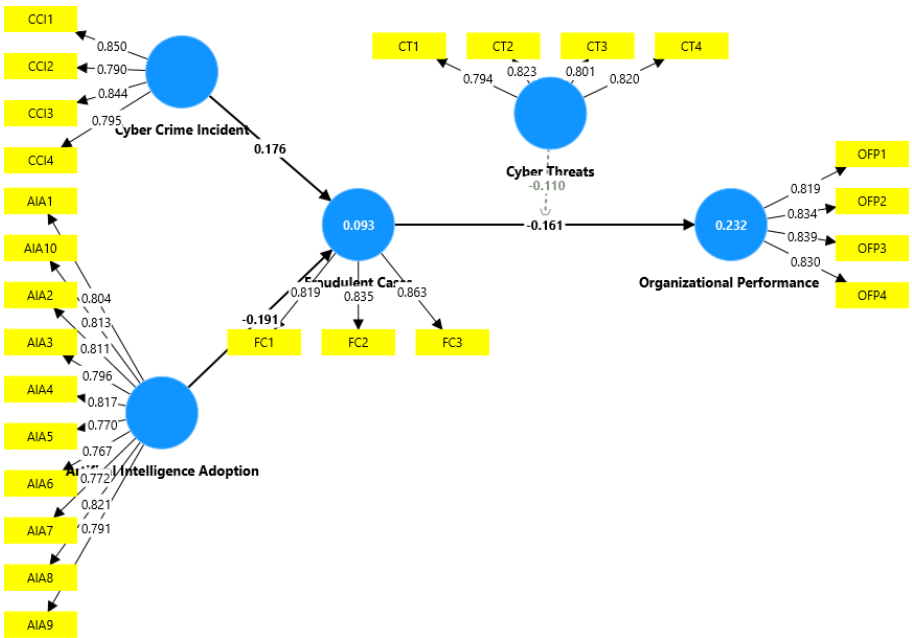

Figure 3: Measurement Model

Convergent validity was tested using the AVE (average variance extracted) criterion as proposed by Fornell and Larcker (1981), with all AVE scores exceeding the 0.5 benchmark (Chin, 1998; Hair et al., 2017). Discriminant validity was further evaluated by examining the heterotrait-monotrait (HTMT) ratio, cross-loadings, and the Fornell-Larcker criterion (Fornell & Larcker, 1981; Hair et al., 2017; Henseler et al., 2015)

Table 1: Reliability and Validity Statistics

Construct	Items	Loading	α	Composite Reliability	AVE
Artificial Intelligence Adoption	AIA1	0.804	0.936	0.941	0.634
	AIA10	0.813			
	AIA2	0.811			
	AIA3	0.796			
	AIA4	0.817			
	AIA5	0.770			
	AIA6	0.767			
	AIA7	0.772			
	AIA8	0.821			
	AIA9	0.791			
Cyber Crime Incident	CCI1	0.850	0.838	0.845	0.673

	CCI2	0.790			
	CCI3	0.844			
	CCI4	0.795			
Cyber Threats	CT1	0.794	0.825	0.828	0.655
	CT2	0.823			
	CT3	0.801			
	CT4	0.820			
Fraudulent Cases	FC1	0.819	0.793	0.812	0.705
	FC2	0.835			
	FC3	0.863			
Organizational Performance	OFP1	0.819	0.850	0.852	0.690
	OFP2	0.834			
	OFP3	0.839			
	OFP4	0.830			

Second, discriminant validity was tested by ensuring that the square root of the average variance extracted (AVE) for each structural equation model construct was greater than its correlations with other constructs, following the Fornell-Larcker criterion. As presented in Table II, these correlations among constructs remained lower than the AVE square root values for each latent variable. Table III demonstrates that the HTMT values were below 1, consistent with Hair et al.'s (2017) recommendations. Additional confirmation of discriminant validity was provided by confirming that each item displayed its highest loading on its intended construct without higher loadings on others. These results validate the reliability and validity standards across all analyzed measurement models.

Table 2: Fornell-Larcker Test

	1	2	3	4
Artificial Intelligence Adoption				
Cyber Crime Incident	0.421			
Cyber Threats	0.505	0.498		
Fraudulent Cases	0.290	0.295		
Organizational Performance	0.998	0.389	0.302	

Table 3: Heterotrait–Monotrait (HTMT) Ratio

	1	2	3	4
Artificial Intelligence Adoption	0.796			
Cyber Crime Incident	-0.374	0.820		
Cyber Threats	-0.445	0.415		
Fraudulent Cases	-0.257	0.248	0.839	
Organizational Performance	0.891	-0.331	-0.254	0.831

The next step, as outlined in Figure III, involved using bootstrapping for structural model estimation. Initially, the variance inflation factor (VIF) was assessed to address potential collinearity issues (Hair et al., 2017). The results showed no collinearity concerns, with VIF scores below 5. The findings demonstrate the examined structural model's strong explanatory ability, with a cybercrime incident and artificial intelligence adoption for fraudulent cases R2 of 0.093, which is weak explanatory power; further, all predictors explained the explanatory power in organizational performance R2 of 0.232, which is medium explanatory power (Hair et al., 2017).

Table 4: R2

	R^2	T Stat	P Values
Fraudulent Cases	0.093	3.802	0.000
Organizational Performance	0.232	7.204	0.000

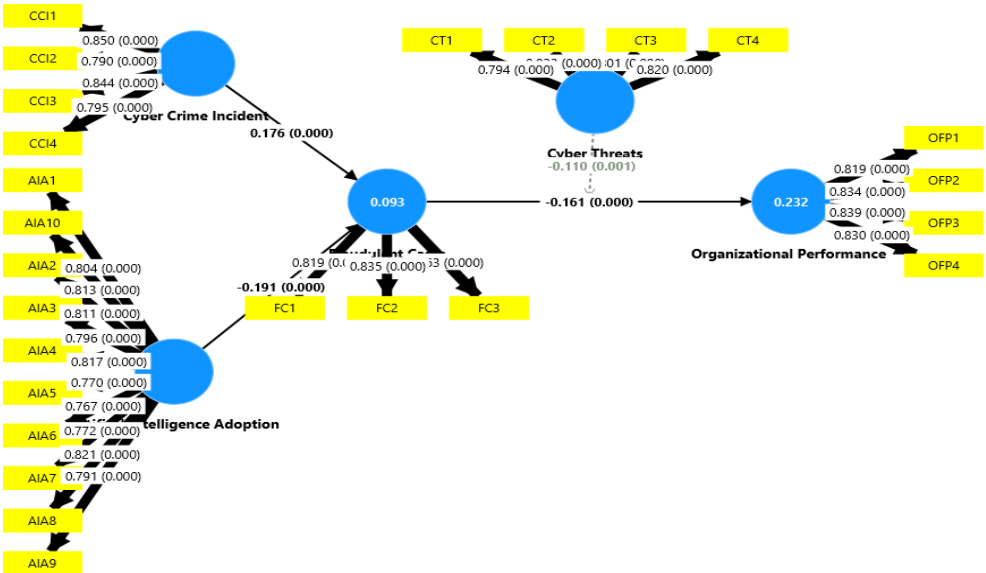

Figure 3: Structural Model

Table 5: Hypothesis Testing

Path	β	S. error	t-value	p-value	Decisions	Confidence Interval	
						2.50%	97.50%
Artificial Intelligence Adoption → Fraudulent Cases	-0.191	0.042	4.516	0.000	Supported	-0.274	-0.108
Artificial Intelligence Adoption → Organizational Performance	0.031	0.014	2.196	0.028	Supported	0.003	0.058
Cyber Crime Incident → Fraudulent Cases	0.176	0.048	3.652	0.000	Supported	0.082	0.271
Cyber Crime Incident → Organizational Performance	-0.028	0.010	2.791	0.005	Supported	-0.048	-0.008
Cyber Threats → Organizational Performance	-0.411	0.037	11.106	0.000	Supported	-0.484	-0.338
Fraudulent Cases → Organizational Performance	-0.161	0.040	3.987	0.000	Supported	-0.240	-0.082
Artificial Intelligence Adoption → Fraudulent Cases → Organizational Performance	0.031	0.014	2.196	0.028	Supported	0.003	0.058
Cyber Crime Incident → Fraudulent Cases → Organizational Performance	-0.028	0.010	2.791	0.005	Supported	-0.048	-0.008
Cyber Threats x Fraudulent Cases → Organizational Performance	-0.110	0.034	3.222	0.001	Supported	-0.177	-0.043

Furthermore, Table v shows that H1 is supported since the suggested relationship between artificial intelligence adoption and fraudulent cases is negative and significant (β= -0.191; t=4.516; p<0.05). Similarly, for H2, artificial intelligence adoption is positively and significantly linked with organizational performance (β= 0.031; t=2.196; p=0.000). Further, cybercrime incidents are positively and significantly linked with fraudulent cases (β= -0.176; t=3.652; p<0.05). Additionally, the cybercrime incident negatively affects organizational performance (β = -0.411; t-value = 11.106; p<0.001). The fraudulent cases have a negative relationship with organizational

performance (β = -0.161; t-value = 3.987; p<0.001). Moreover, cyber threats strengthen the relationship between fraudulent cases and organizational performance from β = -1.161 to β = -0.110.

5 Conclusion

While cybersecurity risks have risen in Pakistan's financial sector, payment and settlement systems have not faced any major disruptions that would hurt the participants' trust, and such risks remain manageable. The State Bank of Pakistan (SBP), which regulates the banking sector and the payment infrastructure, continues to remain extremely vigilant about cyber threats. The SBP understands the increasing digitalization of banking and its attendant risks, so it only engages with banks to improve their defences and resilience, considering such risks. First, the Central Bank of Pakistan has taken several initiatives to prevent banks from vulnerabilities stemming from banks' reliance on third-party service providers by implementing the Framework for Risk Management in Outsourcing Arrangements by Financial Institutions (State Bank of Pakistan, 2017).

SBP has issued broad guidelines for preventing such attacks and for banks to continue improving cybersecurity. This ensures that banks can not only prepare for future cyberattacks but also resist them and then recognise and respond to them if need be. To achieve this objective, banks must integrate the above areas by implementing IT risk management backed by comprehensive standard operating procedures to defend against threats and vulnerabilities of financial information. The SBP has issued Regulations for Payment Card Security to enhance the security of payment cards in Pakistan. These regulations assist card service providers (CSPs) in creating a security framework based on global standards. One of them is that all cards issued must be EMV compliant. EMV standards have been mandated for all cards issued since June 30, 2018. This compliance is essential in protecting customers from fraudulent activities like card skimming. In view of the high Internet banking usage, the SBP has also formulated Regulations for the Security of Internet Banking. These make it obligatory for banks to develop an overarching security framework while emphasizing the need to make staff and customers aware of identity theft and fraud prevention measures. Also, the Government of Pakistan is working on many initiatives to counter the threat of Cybersecurity, showing the national focus on securing digital systems.

The Prevention of Electronic Crimes Act came into effect in Pakistan in 2016, marking a move in the positive direction pertaining to cybercrime laws. The legislation provides an organized method of inspecting, prosecuting, and trying electronic crimes, offences such as cyber-attacks, etc. The government also set up the National Response Centre for Cyber Crime (NR3C) under the Federal Investigation Agency (FIA) to strengthen this legal framework. The NR3C has a mandate for all things tech abuse, which means they will be responding to incidents, working directly to support victims, coordinating the national response and combating cyber-enabled crime. Pakistan has been trying diligently to bring its cyber world in shape, and this collective action indicates the state's endeavours to strengthen cyberspace and digitally protect its citizens. These cybersecurity challenges will need to be addressed urgently by the global community since the financial sector is at the heart of any economy. It is important to make financial institution staff and customers aware of strengthening defences. Furthermore, regulators need to work with the financial sectors to guarantee appropriate cyber defence measures are in place. Given the cross-border nature of cyber-attacks, international cooperation among states, supervisory bodies, law enforcement agencies, and financial institutions is crucial for effectively managing and mitigating the risks associated with these incidents.

The ability of scam callers to convincingly pose as bank employees, often by providing personal information about their targets, raises significant concerns regarding the sources of this data. In Pakistan, the absence of robust data protection laws and a coherent cybercrime policy has created an environment where gangs of scammers exploit the digital illiteracy prevalent among the population. But how do these criminals obtain individuals' personal and banking details to execute

their schemes? Reports indicate that numerous groups on platforms like Facebook are selling data from the National Database and Registration Authority (Nadra), including family trees, SIM and phone records, and location information. Asif Iqbal, Deputy Director of the Federal Investigation Agency (FIA) Cyber Crime unit, has noted that many lists of mobile numbers have been leaked online and remain publicly accessible. Furthermore, data from national and provincial social safety net programs, such as the Benazir Income Support Programme (BISP), is also allegedly being misused, according to Iqbal. The Ministry of Information Technology and Telecommunication did not respond to inquiries regarding these claims.

On June 25, 2023, the Federal Investigation Agency (FIA) announced a crackdown on a gang operating in Gujranwala that posed as courier company staff. These criminals would request thumbprints from individuals receiving courier deliveries, which they then reproduced on special paper. This fraudulent method allowed them to activate cellular phone SIM cards in the victims' names. Once the SIMs were activated, they would use them to access banking apps and withdraw funds. During the investigation, gang members revealed they received the necessary personal information from an individual affiliated with a "bank data gang." Notably, one of the suspects involved in this scheme held a position as a branch manager at a private bank.

Asif Iqbal, Deputy Director of Cyber Crime at the FIA, highlights that data theft and misuse have become systemic issues within Pakistan's digital banking sector. Initially, a group of petty criminals engaged in small-scale phone banking scams has evolved into a more organized operation. These criminals are primarily located in various cities across Punjab, including Sargodha, Jhang, Chiniot, Pindi Bhattian, Hafizabad, Gujrat, Chichawatni, Layyah, and Sheikhupura. Iqbal notes that the leaders of these operations have accumulated significant wealth, evidenced by their mansions, which cover about four kanals (approximately 2,000 square meters), along with expensive vehicles. Many individuals the author interviewed reported receiving scam calls from regular cell phone numbers, further indicating the pervasive nature of this problem.

Criminals operate with a sense of impunity, believing they can scam individuals without consequence, largely due to the significant political power they have accumulated over time. They often receive warnings if the FIA plans a raid, allowing them to evade capture. Authorities have faced attacks during attempts to conduct operations against these criminals. The strategies employed in these scams are deceptively simple: they target the vulnerabilities of the poor, naïve, uneducated, and fearful. For instance, consider a scenario where a woman, struggling financially, purchases a SIM card. The shopkeeper requests her thumbprint under the pretense of a connectivity issue, misleading her into thinking the SIM cannot be activated immediately. He then sells that SIM to fraudsters while activating a new one using the information she provided—iqbal points out a network of such dishonest shopkeepers and franchise owners. When the FIA traces the SIM back to the franchise for questioning, the criminals are often already forewarned and have fled the scene, making it increasingly difficult for authorities to apprehend them.

Criminals operate with a sense of freedom in scamming individuals despite the ease with which authorities can trace phone numbers. This confidence stems from the significant political power they have accumulated over time, often receiving advance warnings about impending raids by the FIA. There have been instances where authorities faced violent resistance when attempting to conduct operations against these criminals. The tactics employed in these scams are notably straightforward: they prey on the vulnerabilities of the poor, naïve, uneducated, and fearful. For instance, consider a scenario where a financially struggling woman visits a shop to purchase a SIM card. The shopkeeper requests her thumbprint under false pretenses, claiming a connectivity issue prevents immediate activation. Fraudsters have developed a scheme where they exploit individuals' personal information to commit identity theft. In one example of this type, the scammer gets hold of a woman's username and password to activate a new SIM card in her name and sells her original SIM card to other criminals. This operation involves a circle of deceitful

shopkeepers and franchise holders involved in these tricks, as per Iqbal. However, criminals are usually alerted when the Federal Investigation Agency (FIA) traces the suspicious SIM card back to the shop where it was obtained to question the owner. The situation highlights the immensity of law enforcement's difficulty with organized cybercrime.

However, this demonstrates that it is clearer than ever that a way to prevent this is through tighter regulations and better enforcement of SIM card sales. Beefing up these steps could really help officials catch such scams and prosecute the people behind the schemes.

5.1 Managerial Implications

With the rapid development of technology and criminals adapting new methods to commit their crimes, fighting cybercrime remains a serious issue. In response, worldwide governments and organizations have come up with remedies such as firewalls to block attacks, filter and ward off malware, and routine IT staff training to recognize anomalous traffic and detect intrusions. It is important to pass stringent laws and punish the offenders as a deterrent; at the same time, organizations need to implement secure user access front doors so that only those authorized can access the network. Additional solutions include keeping software and applications updated per global best practices and encouraging cooperation amongst banking institutions (for example, many fraudsters shift funds illegitimately through various accounts). For banks, a collective response can allay the potential risks posed by these cyber implications by improving security and safeguarding consumers against the threat of swindlers who rely on social postings for fake news and premeditated fraud.

All institutions must cooperate when detecting fraudulent transfers to combat fraud effectively. Still, there is a need to broaden public awareness of fraud and provide consumers with knowledge on navigating critical digital use cases safely. Education is essential to reinforce digital literacy and safety. Seminars and cyber safety workshops should be arranged occasionally to teach people how to safeguard their personal information. These should focus on such protocols as installing specific anti-malware software on devices and avoiding pirated software, which can allow viruses into systems. Individuals should never share their PIN, bank account details, or email access with strangers, as this compromises security. Additionally, avoiding sharing sensitive data is crucial, as no network is completely safe from cyber threats. Unsolicited emails or SMS messages asking for financial details should be ignored, as these are often phishing attempts. To mitigate and prevent cybercrimes, the private and public sectors must invest more in cybersecurity to protect vital sectors like health and the economy and avoid excessive spending on countering these threats. Ultimately, the best defense is raising awareness and educating people.

Hassan et al. (2012) pointed out that property owners are more likely to protect their property and property rights when laws encourage such behaviour. Similarly, entities with extensive network infrastructures must adopt solid measures to protect networks, data, and systems from cybercrime. Financial institutions and businesses should prioritize several key actions to reduce cybercrime effectively. Regular user awareness programs are essential for educating employees on the importance of cybersecurity while developing and enforcing policies that create a strong IT environment is critical for smooth operations. Additionally, conducting Vulnerability Assessment and Penetration Testing on large data infrastructures can help identify and address potential weaknesses. Securing insurance coverage for potential losses due to cybercrime is also beneficial. Collaborative efforts, such as sharing information about the nature, sources, and frequency of cyber-attacks, enhance collective defences. Finally, organizing workshops to build capacity among the public and security personnel provides them with proactive and sustainable approaches to combat cybercrime effectively.

5.2 Limitations

Although studies based on artificial intelligence for bank fraud detection provide valuable

insights, they focus solely on detecting fraudulent transactions within online banking. Detecting other types of financial fraud may require different methods. Additionally, the limited sample size within the financial sector may restrict the robustness and generalizability of the findings. Another issue is that human biases during data selection and analysis can impact the overall dependability and validity of the methodology.

6 References:

Akram, M. S., Mir, M. J., & Rehman, A. (2023). Dimension of cyber-warfare in Pakistan's context. *Journal of Positive School Psychology*, *7*(6), 82–94.

Aksa, A. F., Irianto, B. S., & Bawono, I. R. (2020). The urgency of rationalization for unethical behavior and accounting fraud. *Jurnal Akuntansi Multiparadigma*, *11*(3), 653–664.

Akwara, A. F., Akwara, N. F., Enwuchola, J., Adekunle, M., & Udaw, J. E. (2021). Unemployment and poverty: Implications for national security and good governance in Nigeria. *ESCET Journal of Educational Research and Policy Studies*, *1*(2), 244–256.

Alghamdi, W., & Schukat, M. (2020). Cyber attacks on precision time protocol networks—A case study. *Electronics*, *9*(9), Article e1398. https://doi.org/10.3390/electronics9091398

Alhaddad, M. M. (2018). Artificial intelligence in banking industry: A review on fraud detection, credit management, and document processing. *ResearchBerg Review of Science and Technology*, *2*(3), 25–46.

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access*, *8*, 137293–137311. https://doi.org/10.1109/ACCESS.2020.3011259

Alqethami, S., Almutanni, B., & AlGhamdi, M. (2021). Fraud detection in E-commerce. *International Journal of Computer Science & Network Security*, *21*(6), 312–318.

Arenas, Á., Ray, G., Hidalgo, A., & Urueña, A. (2024). How to keep your information secure? Toward a better understanding of users security behavior. *Technological Forecasting and Social Change*, *198*, Article e123028. https://doi.org/10.1016/j.techfore.2023.123028

Arkorful, V. E., Lugu, B. K., Arkorful, V. A., & Charway, S. M. (2022). Probing the predictors of fraud using the fraud diamond theory: An empirical evidence from local governments in Ghana. *Forum for Development Studies*, *49*(2), 291–318. https://doi.org/10.1080/08039410.2022.2080759

Arora, S., & Bhatia, M. (2022). Challenges and opportunities in biometric security: A survey. *Information Security Journal: A Global Perspective*, *31*(1), 28–48. https://doi.org/10.1080/19393555.2021.1873464

Arshad, N., Ahmad, W., & Manzoor, K. (2024, September 3–4). *Unleashing the potential of Pakistan's it industry: Building for massive software export growth* [Conference paper]. Proceedings of 4th RASTA conference. Islamabad, Pakistan.

Bagozzi, R. P., Yi, Y., & Phillips, L. W. (1991). Assessing construct validity in organizational research. *Administrative science quarterly*, *36*(3), 421–458.

Beju, D.-G., & Făt, C.-M. (2023). Frauds in Banking System: Frauds with Cards and Their Associated Services. In M. V. Achim, & S. N. Borlea (Eds.), *Economic and Financial Crime, Sustainability and Good Governance* (pp. 31–52). Springer.

Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer Science & IT Research Journal*, *5*(6), 1505–1520. https://doi.org/10.51594/csitrj.v5i6.1252

Beyari, H. (2021). Recent e-commerce trends and learnings for e-commerce system development from a quality perspective797–810. *International Journal for Quality Research*, *15*(3), 797–810. https://doi.org/10.24874/IJQR15.03-07

Bhakhri, K., Sethi, M., Sharma, I., & Kaushik, K. (2023, November 29–30). *Examining the consequences of cyberattacks on businesses and organizations* [Paper presentation]. International Conference on Innovations in Data Analytics. West Bengal, India

Bido, D., da Silva, D., & Ringle, C. (2014). Structural equation modeling with the SmartPLS.

Brazilian Journal of Marketing, *13*(2), 56–73.

Blythe, J. M., & Johnson, S. D. (2021). A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal*, *34*, 97–125. https://doi.org/10.1057/s41284-019-00211-8

Bukht, T. F. N., Raza, M. A., Awan, J. H., & Ahmad, R. (2020b). Analyzing cyber-attacks targeted on the Banks of Pakistan and their Solutions. *International Journal of Computer Science and Network Security*, *20*(2), 31–38.

Cavaliere, L. P. L., Subhash, N., Durga Rao, P. V., Mittal, P., Koti, K., Chakravarthi, M. K., & Regin, R. (2021). The Impact of Internet Fraud on Financial Performance of Banks. *Turkish Online Journal of Qualitative Inquiry*, *12*(6), 8126–8158.

Chen, H., He, M., & Peng, L. (2024). Understanding online shopping fraud among Chinese elderly: Extending routine activity theory in the online context. *Telematics and Informatics*, *96*, Article e102208. https://doi.org/10.1016/j.tele.2024.102208

Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling. *MIS Quarterly*, *22*(1), 7–16.

Clinton, L. (2023). *Fixing American cybersecurity: Creating a strategic public-private partnership*. Georgetown University Press.

Crowther, D., & Lancaster, G. (2012). *Research methods*. Routledge.

Dorminey, J., Fleming, A. S., Kranacher, M. J., & Riley Jr, R. A. (2012). The evolution of fraud theory. *Issues in Accounting Education*, *27*(2), 555–579. https://doi.org/10.2308/iace-50131

Duarte, P. A. O., & Raposo, M. L. B. (2010). A PLS model to study brand preference: An application to the mobile phone market. In V. E. Vinzi, W. W. Chin, J. & Henseler, H. Wang (Eds.), *Handbook of partial least squares: Concepts, methods and applications*, (pp. 449–485). Springer.

Ene, W. R., & Imo, A. S. (2024). Cybercrime and its implications for human capital development: A study of Otuoke Community, Fuo Students. *Fuoye Journal Of Criminology And Security Studies*, *3*(2), 53–75.

Firdaus, R., Xue, Y., Gang, L., & Sibt e Ali, M. (2022). Artificial intelligence and human psychology in online transaction fraud. *Frontiers in Psychology*, *13*, Article e947234. https://doi.org/10.3389/fpsyg.2022.947234

Fornell, C., & Larcker, D. F. (1981). *Structural equation models with unobservable variables and measurement error: Algebra and statistics*. Sage Publications.

Franjić, S. (2020). Cybercrime is very dangerous form of criminal behavior and cybersecurity. *Emerging Science Journal*, *4*(18), 18–26. http://dx.doi.org/10.28991/esj-2020-SP1-02

Gautam, A. (2023). The evaluating the impact of artificial intelligence on risk management and fraud detection in the banking sector. *AI, IoT and the Fourth Industrial Revolution Review*, *13*(11), 9–18.

Gayam, S. R. (2020). AI-Driven fraud detection in e-commerce: Advanced techniques for anomaly detection, transaction monitoring, and risk mitigation. *Distributed Learning and Broad Applications in Scientific Research*, *6*, 124–151.

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). *Cyber security threats, vulnerabilities, and security solutions models in banking*. Authorea Preprints. https://www.authorea.com/doi/full/10.22541/au.166385206.63311335

Gilani, S. R. S., Mujtaba, B. G., Zahoor, S., & AlMatrooshi, A. M. (2023). Exploring cybercrime history through a typology of computer mediated offences: Applying Islamic principles to promote good and prevent harm. *Computing and Artificial Intelligence*, *1*(1), 321–321. https://doi.org/10.59400/cai.v1i1.321

Goni, O., Ali, M. H., Showrov, M. M. A., & Shameem, M. A. (2022). The basic concept of cyber crime. *Journal of Technology Innovations and Energy*, *1*(2), 16–24.

Gottschalk, P., & Hamerton, C. (2021). *White-collar crime online: Deviance, organizational*

behaviour and risk. Springer Nature.

Graham, A. (2023). *Cybercrime: Traditional problems and modern solutions* [Doctoral dissertation, Te Herenga Waka-Victoria University of Wellington]. https://openaccess.wgtn.ac.nz/articles/thesis/Cybercrime_Traditional_Problems_and_Modern_Solutions/22300909?file=39669757

Haider, A., Yousaf, U., Shah, N. H., & Azeem, W. (2024). UNTOC's role in combating transnational organized crime: An international response. *Pakistan Journal of Law, Analysis and Wisdom*, *3*(8), 178–188.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). Sage.

Haque, E. U., Abbasi, W., Murugesan, S., Anwar, M. S., Khan, F., & Lee, Y. (2023). Cyber forensic investigation infrastructure of Pakistan: An analysis of the cyber threat landscape and readiness. *IEEE Access*, *11*, 40049–40063. https://doi.org/10.1109/ACCESS.2023.3268529

Hassan, A. B., Lass, F. D., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, effects and the way out. *ARPN Journal of Science and Technology*, *2*(7), 626–631.

Hassan, M., Aziz, L. A.-R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: An exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, *6*(1), 110–132.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert systems with Applications*, *193*, Article e116429. https://doi.org/10.1016/j.eswa.2021.116429

Huan, Y., & Qamruzzaman, M. (2022). Innovation-led FDI sustainability: clarifying the nexus between financial innovation, technological innovation, environmental innovation, and FDI in the BRIC nations. *Sustainability*, *14*(23), Article e15732. https://doi.org/10.3390/su142315732

Ibrahim, H. (2022). A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies. *Wasit Journal of Computer and Mathematics Science*, *1*(3), 50–68. https://doi.org/10.31185/wjcm.48

Iftikhar, S. (2024). Cyberterrorism as a global threat: A review on repercussions and countermeasures. *PeerJ Computer Science*, *10*, Article e1772. https://doi.org/10.7717/peerj-cs.1772

Jansen, J., & Leukfeldt, R. (2015, July 13). *How people help fraudsters steal their money: An analysis of 600 online banking fraud cases* [Paper presentation]. Proceeding of 2015th workshop on socio-technical aspects in security and trust. Verona, Italy

Javaid, H. A. (2024). Improving fraud detection and risk assessment in financial service using predictive analytics and data mining. *Integrated Journal of Science and Technology*, *1*(8), 1–11.

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*, Article e100016. https://doi.org/10.1016/j.csa.2023.100016

Kafetzopoulos, D., & Psomas, E. (2015). The impact of innovation capability on the performance of manufacturing companies: The Greek case. *Journal of Manufacturing Technology Management*, *26*(1), 104–130. https://doi.org/10.1108/JMTM-12-2012-0117

Kagias, P., Cheliatsidou, A., Garefalakis, A., Azibi, J., & Sariannidis, N. (2022). The fraud triangle–an alternative approach. *Journal of Financial Crime*, *29*(3), 908–924.

https://doi.org/10.1108/JFC-07-2021-0159

Kao, D.-Y. (2020, Febuaray 16–19). *Comprehending Taiwan ATM heist: From cyber-attack phases to investigation processes* [Paper presentation]. 2020 22nd International Conference on Advanced Communication Technology (ICACT). Phoenix Park, South Korea.

Kazemian, S., Said, J., Hady Nia, E., & Vakilifard, H. (2019). Examining fraud risk factors on asset misappropriation: Evidence from the Iranian banking industry. *Journal of Financial Crime*, *26*(2), 447–463. https://doi.org/10.1108/JFC-01-2018-0008

Ketenci, U. G., Kurt, T., Önal, S. m., Erbil, C., Aktürkoğlu, S. n., & İlhan, H. Ş. (2021). A time-frequency based suspicious activity detection for anti-money laundering. *IEEE Access*, *9*, 59957–59967. https://doi.org/10.1109/ACCESS.2021.3072114

Khalil, B. (2020, March 22). *Cybercrime affecting banking sector economy of Pakistan*. Modern Diplomacy. https://moderndiplomacy.eu/2020/03/22/cybercrime-effecting-banking-sector-economy-of-pakistan/

Khan, M. F., Raza, A., & Naseer, N. (2021). Cyber security and challenges faced by Pakistan. *Pakistan Journal of International Affairs*, *4*(4), 865–881. https://doi.org/10.52337/pjia.v4i4.408

Khan, M. I., Arif, A., & Khan, A. R. A. (2024). The Most Recent Advances and Uses of AI in Cybersecurity. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(4), 566–578.

Khattak, S., Jan, S., Ahmad, I., Wadud, Z., & Khan, F. Q. (2021). An effective security assessment approach for Internet banking services via deep analysis of multimedia data. *Multimedia Systems*, *27*, 733–751. https://doi.org/10.1007/s00530-020-00680-7

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, *26*, 89–120. https://doi.org/10.1007/s11948-018-00081-0

Klenowski, P. M., & Copes, H. (2020). Looking back at other people's money: A qualitative test of cressey's classic hypothesis of trust violating behavior. *Journal of Qualitative Criminal Justice & Criminology*, *1*(1), 1–24 https://doi.org/10.21428/88de04a1.9f45b3c4

Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal*, *28*(1), 227–261. https://doi.org/10.1111/isj.12131

Kokaji, A., & Goto, A. (2022). An analysis of economic losses from cyberattacks: Based on input–output model and production function. *Journal of Economic Structures*, *11*(1), 34.

Kumar, T., Bhushan, S., Sharma, P., & Garg, V. (2024). Examining the vulnerabilities of biometric systems: Privacy and security perspectives. In A. Selwal, D. Sharma, M. Mann, S. Chakraborty, V. E. Balas, O. E. Lieh (Eds.), *Leveraging computer vision to biometric applications* (pp. 34–67). Chapman and Hall/CRC.

Mohammed, A. F. A., & Rahman, H. M. A. A. (2024). The role of artificial intelligence (AI) on the fraud detection in the private sector in Saudi Arabia. *Journal of Arts, Literature, Humanities and Social Sciences*, *100*, 472–506. https://doi.org/10.33193/JALHSS.100.2024.1018

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current psychiatry reports*, *23*, 1–9. https://doi.org/10.1007/s11920-021-01228-w

Mostafa, A. A. (2022). Cyber Crime in Business. *International Journal of Academic Research in Business and Social Sciences.*, *12*(6), 962–972.

Muhammad, T., Munir, M. T., Munir, M. Z., & Zafar, M. W. (2022). Integrative cybersecurity: Merging zero trust, layered defense, and global standards for a resilient digital future. *International Journal of Computer Science and Technology*, *6*(4), 99–135.

Mytnyk, B., Tkachyk, O., Shakhovska, N., Fedushko, S., & Syerov, Y. (2023). Application of artificial intelligence for fraudulent banking operations recognition. *Big Data and*

Cognitive Computing, *7*(2), Article e93. https://doi.org/10.3390/bdcc7020093

Nicholls, J., Kuppa, A., & Le-Khac, N.-A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access*, *9*, 163965–163986. https://doi.org/10.1109/ACCESS.2021.3134076

Nicholson, J., Terry, J., Beckett, H., & Kumar, P. (2021, October 11–12). *Understanding young people's experiences of cybersecurity* [Paper presentation]. Proceedings of the 2021 European Symposium on Usable Security. Karlsruhe, Germany.

Nikolopoulou, K. (2022). Face-to-face, online and hybrid education: University students' opinions and preferences. *Journal of Digital Educational Technology*, *2*(2), Article eep2206. https://doi.org/10.30935/jdet/12384

Onwunyi, U. M., & Okonkwo, K. J. (2021). Youth and cybercrime in nigeria: Implications of the nationwide covid 19 lockdown. *International Journal of Legal Studies*, *10*(2), 209–232. https://doi.org/10.5281/zenodo.5865939

Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. *Crime, Law and Social Change*, *70*, 397–420. https://doi.org/10.1007/s10611-018-9774-y

Pasculli, L. (2020). The Global Causes of Cybercrime and State Responsibilities: Towards an Integrated Interdisciplinary Theory. *Journal of Ethics and Legal Technologies 2*(1), 48–74.

Rahman, M., Ming, T. H., Baigh, T. A., & Sarker, M. (2023). Adoption of artificial intelligence in banking services: An empirical analysis. *International Journal of Emerging Markets*, *18*(10), 4270–4300. https://doi.org/10.1108/IJOEM-06-2020-0724

Riaz, A., Ramay, S. A., Abbas, F., Hussain, A., Naveed, N., & Abbas, T. (2024). Analyzing the Impact of Cybercrime and Its Security in Banking Sectors of Pakistan by Using Data Mining. *Journal of Computing & Biomedical Informatics*, *8*(1), Article e747. https://doi.org/10.56979/801/2024

Rodrigues, V. F., Policarpo, L. M., da Silveira, D. E., da Rosa Righi, R., da Costa, C. A., Barbosa, J. L. V., Antunes, R. S., Scorsatto, R., & Arcot, T. (2022). Fraud detection and prevention in e-commerce: A systematic literature review. *Electronic Commerce Research and Applications*, *56*, Article e101207. https://doi.org/10.1016/j.elerap.2022.101207

Romanchuk, J. (2024, November 25). *The four types of research design—everything you need to know*. https://blog.hubspot.com/marketing/types-of-research-design

SailPoint. (2021, March 6). *Top 5 banking fraud prevention methods*. https://www.sailpoint.com/identity-library/top-5-banking-fraud-prevention-methods/

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), 202–209.

Salameh, R., & Lutfi, K. (2021). The role of artificial intelligence on limiting Jordanian commercial banks cybercrimes. *Accounting*, *7*(5), 1147–1156. http://dx.doi.org/10.5267/j.ac.2021.2.024

Saleem, B., Ahmed, M., Zahra, M., Hassan, F., Iqbal, M. A., & Muhammad, Z. (2024). A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap. *International Cybersecurity Law Review*, 5, 533–561. https://doi.org/10.1365/s43439-024-00128-y

Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. *SN computer science*, *2*(3), Article e160. https://doi.org/10.1007/s42979-021-00592-x

Shetty, A. A., & Murthy, K. V. (2023). Investigation of card skimming cases: An Indian Perspective. *Journal of Applied Security Research*, *18*(3), 519–532. https://doi.org/10.1080/19361610.2021.2024049

Shulzhenko, N., & Romashkin, S. (2020). Internet fraud and transnational organized crime. *Juridical Tribune*, *10*(1), 162–172.

Sohel, A., Alam, M. A., Waliullah, M., Siddiki, A., & Uddin, M. M. (2024). Fraud detection in financial transactions through data science for real-time monitoring and prevention. *Academic Journal on Innovation, Engineering & Emerging Technology*, *1*(01), 91–107. https://doi.org/10.69593/ajieet.v1i01.132

State Bank of Pakistan. (2017, June 20). *BPRD circular no. 06 of 2017*. http://www.sbp.org.pk/bprd/2017/C6.htm

Sultan, N., & Mohamed, N. (2023). The role of information sharing in combating money laundering: The importance and challenges of mutual legal assistance for developing jurisdictions like Pakistan. *Journal of Money Laundering Control*, *26*(6), 1242–1260. https://doi.org/10.1108/JMLC-09-2022-0128

Tahir, M., Farrukh, T., & Shahid, M. (2019). Cyber laws and cyber security in Pakistan: Myths and realities. *Global Social Sciences Review*, *4*(1), 485–493.

Tickner, P., & Button, M. (2021). Deconstructing the origins of Cressey's Fraud Triangle. *Journal of Financial Crime*, *28*(3), 722–731. https://doi.org/10.1108/JFC-10-2020-0204

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Management*, *22*(4), 239–309. https://doi.org/10.1057/s41283-020-00063-2

Ullah, F., Ali, A., & Umar, Z. (2021). Understanding cybercrime and youth: A perception based approach. *Pakistan Journal of Social Research*, *3*(3), 130–136.

Vousinas, G. L. (2019). Advancing theory of fraud: The SCORE model. *Journal of Financial Crime*, *26*(1), 372–381. https://doi.org/10.1108/JFC-12-2017-0128

Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age*. John Wiley & Sons.

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. *IEEE Access*, *8*, 146598–146612. https://doi.org/10.1109/ACCESS.2020.3013145

Wolfe, D. T. & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *CPA Journal*, *74*(12), 38–42.

Xia, Q., Chiu, T. K., Lee, M., Sanusi, I. T., Dai, Y., & Chai, C. S. (2022). A self-determination theory (SDT) design approach for inclusive and diverse artificial intelligence (AI) education. *Computers & Education*, *189*, Article e104582. https://doi.org/10.1016/j.compedu.2022.104582

Yeboah-Ofori, A., & Opoku-Boateng, F. A. (2023). Mitigating cybercrimes in an evolving organizational landscape. *Continuity & Resilience Review*, *5*(1), 53–78. https://doi.org/10.1108/CRR-09-2022-0017