AMERICAN INTERNATIONAL UNIVERSITY-BANGLADESH

Faculty of Science and Technology

Assignment Cover Sheet

Assignment Title:	Mid Assignment		
Assignment No:	01	Date of Submission:	13 July 2023
Course Title:	Research Methodology		
Course Code:	CSC4197	Section:	C
Semester:	Summer 2022-23	Course Teacher:	DR. MD. ABDULLAH - AL - JUBAIR

Declaration and Statement of Authorship:

1. I/we hold a copy of this Assignment/Case-Study, which can be produced if the original is lost/damaged.
2. This Assignment/Case-Study is my/our original work and no part of it has been copied from any other student's work or from any other source except where due acknowledgement is made.
3. No part of this Assignment/Case-Study has been written for me/us by any other person except where such collaboration has been authorized by the concerned teacher and is clearly acknowledged in the assignment.
4. I/we have not previously submitted or currently submitting this work for any other course/unit.
5. This work may be reproduced, communicated, compared and archived for the purpose of detecting plagiarism.
6. I/we give permission for a copy of my/our marked work to be retained by the faculty for review and comparison, including review by external examiners.
7. I/we understand that Plagiarism is the presentation of the work, idea or creation of another person as though it is your own. It is a formofcheatingandisaveryseriousacademicoffencethatmayleadtoexpulsionfromtheUniversity. Plagiarized material can be drawn from, and presented in, written, graphic and visual form, including electronic data, and oral presentations. Plagiarism occurs when the origin of them arterial used is not appropriately cited.
8. I/we also understand that enabling plagiarism is the act of assisting or allowing another person to plagiarize or to copy my/our work.

** Student(s) must complete all details except the faculty use part.*
** Please submit all assignments to your course teacher or the office of the concerned teacher.

Group Name/No.:

No	Name	ID	Program	Signature
1	MUNTAQA MALIYAT	20-43248-1	BSc [CSE]	
2	MD. RIYADH SHEIKH	20-42748-1	BSc [CSE]	
3	SAIFUL ISLAM	20-42585-1	BSc [CSE]	
4	MD. SAROAR AZIZ	19-41105-2	BSc [CSE]	
5	ABU ABDULLAH	20-43966-2	BSc [CSE]	

Faculty use only

FACULTYCOMMENTS	**Marks Obtained**	
	Total Marks	

MOBILE BANKING AND FINANCIAL FRAUD IN BANGLADESH

The Topic of Interest:

Mobile banking has revolutionized the way people in Bangladesh manage their finances, providing convenient access to banking services through mobile devices. With the increasing penetration of smartphones and the internet, mobile banking has gained significant popularity in the country, as it offers a convenient and affordable way to access financial services. However, this growth has also led to an increase in financial fraud, as criminals have found new techniques to exploit the vulnerabilities of mobile banking systems. Some of those include such as malware and phishing attacks, SIM card cloning, social engineering, and identity theft to gain unauthorized access to users' financial information and carry out fraudulent transactions. Malware can be disguised as legitimate apps or websites, infecting mobile devices and stealing sensitive data. Phishing attacks involve tricking users into providing personal or financial information through fraudulent communications. SIM card cloning and swapping allow fraudsters to intercept authentication codes and access accounts. Social engineering techniques manipulate users into divulging confidential information through manipulative tactics. According to a recent study by the Bangladesh Bank, one out of every ten mobile banking users in Bangladesh has been a victim of fraud. The most common types of mobile banking fraud include phishing, smishing, and vishing. Phishing is a fraudulent technique where criminals send deceptive emails or text messages that appear to be from legitimate banks or financial institutions. These messages often contain links that direct victims to fake websites mimicking the genuine ones. Once on these fake websites, unsuspecting individuals may unknowingly enter their personal and financial information, which the fraudsters then exploit for illicit purposes. Smishing, a variation of phishing, uses SMS text messages instead of emails to deceive victims. These text messages often contain urgent or enticing messages that prompt recipients to click on malicious links or provide sensitive information. Smishing attacks are particularly successful due to the immediacy and sense of urgency associated with text messages. Among the three types, vishing is a technique that has proven to be particularly effective in deceiving Bangladeshi individuals. Vishing, which stands for "voice phishing," another prevalent mobile banking fraud method, relies on voice calls. Fraudsters impersonate bank representatives or other trusted entities, using social engineering techniques to manipulate victims into revealing confidential information, such as account details or personal identification numbers. Vishing attacks often appear legitimate, as fraudsters can manipulate caller IDs to display legitimate-sounding phone numbers, further deceiving victims into trusting the caller. In order to combat financial fraud, the Bangladesh Bank has issued a number of regulations and guidelines for mobile banking providers. These regulations require mobile banking providers to implement security measures such as two-factor authentication and to educate their customers about the risks of fraud.

Problem of Statement:

The rapid adoption of mobile banking in Bangladesh has brought about a surge in financial fraud cases, posing significant risks to mobile banking users. Various sophisticated techniques, such as phishing attacks, SIM swapping attacks, and malware attacks, have emerged as common methods employed by fraudsters to exploit unsuspecting individuals. Against this backdrop, the primary objective of this research project is to address the critical problem statement: How can the incidence of financial fraud in Bangladesh be effectively reduced, particularly within the context of mobile banking? By investigating and identifying strategies, encompassing user education, enhanced security measures, and regulatory frameworks, this study aims to provide valuable insights and recommendations to combat mobile banking fraud, safeguard user interests, and foster a secure digital financial landscape in Bangladesh.

Primary Research Question:

Based on the problem statement, the primary research question for this project is, what are the most effective strategies for reducing the incidence of financial fraud in Bangladesh, specifically in the context of mobile banking? This aims to investigate the most effective strategies for reducing the incidence of financial fraud in Bangladesh, with a specific focus on the context of mobile banking. This research question seeks to explore and identify strategies that have proven to be successful in mitigating mobile banking fraud within the country. By conducting a comprehensive investigation, the study aims to contribute to the development of practical and targeted approaches to combat financial fraud in the mobile banking sector in Bangladesh. To address this research question, the study will involve examining existing literature, academic research, and well-researched press articles on the subject. This will provide a foundation for understanding the current landscape of financial fraud in Bangladesh and the specific challenges faced in the context of mobile banking. The study will also consider insights from industry experts, regulatory bodies, and relevant stakeholders to gain a comprehensive understanding of the strategies that have been employed and their effectiveness. The research will employ both qualitative and quantitative methods to gather data. Qualitative methods, such as interviews and focus groups, will be conducted with key stakeholders, including representatives from mobile banking providers, regulatory bodies, law enforcement agencies, and customers. These interviews will provide insights into their experiences, perceptions, and recommendations regarding strategies for reducing financial fraud in mobile banking. Additionally, quantitative data will be collected through surveys distributed to a representative sample of mobile banking users in Bangladesh. The survey will explore users' awareness of fraud risks, their experiences with fraud, and their opinions on the effectiveness of various strategies employed by mobile banking providers. The collected data will be analyzed using appropriate statistical techniques and thematic analysis to identify patterns, common themes, and potential correlations. The findings will be synthesized to determine the most effective strategies for reducing financial fraud in the context of mobile banking in Bangladesh. Ultimately, the research aims to provide actionable recommendations to mobile banking providers, regulatory bodies, and policymakers on implementing effective strategies to combat financial fraud. The findings will contribute to enhancing the security and trustworthiness of the mobile banking ecosystem in Bangladesh, ultimately protecting users and promoting the growth of digital financial services in the country.

Two Specific Aims/Objectives:

The two specific aims/objectives for reducing financial fraud in the context of mobile banking in Bangladesh:

1. Evaluate the effectiveness of advanced technological measures in reducing mobile banking fraud:
This aim focuses on assessing how advanced technological measures contribute to reducing the incidence of financial fraud in the mobile banking sector of Bangladesh. To achieve this objective, extensive research and analysis of existing technological solutions deployed by mobile banking service providers are conducted. Firstly, the research involves evaluating the effectiveness of biometrics and multi-factor authentication in ensuring secure access to mobile banking services. Biometric features like fingerprints or facial recognition provide a unique and personalized authentication method, making it difficult for fraudsters to impersonate users. Similarly, multi-factor authentication combines multiple verification factors (such as passwords, one-time codes, or security tokens) to add an extra layer of security. Secondly, encryption protocols and secure communication channels are examined. These measures protect sensitive customer information during transactions, preventing unauthorized access by encrypting data and ensuring its integrity and confidentiality. Additionally, the research analyzes the implementation of real-time fraud detection systems powered by artificial intelligence and machine learning algorithms. These systems continuously monitor transactions, user behavior, and patterns to detect anomalies or suspicious activities that may indicate potential fraud. By swiftly identifying fraudulent transactions or activities, appropriate actions can be taken to mitigate risks and prevent financial losses. The evaluation of these technological measures includes reviewing case studies, analyzing statistical data on fraud incidents, and conducting surveys or interviews with mobile banking stakeholders. By examining their efficacy in preventing unauthorized access, protecting customer information, and detecting fraudulent activities, the research provides insights into the impact of advanced technological measures on reducing financial fraud in Bangladesh's mobile banking sector.

2. Investigate the impact of regulatory frameworks on minimizing mobile banking fraud:
This objective aims to investigate the role and impact of regulatory frameworks in reducing financial fraud in the mobile banking sector of Bangladesh. It involves evaluating the existing regulatory guidelines and standards imposed on mobile banking service providers. The

research examines the extent to which these regulations address fraud prevention measures. This includes analyzing specific requirements for strong customer authentication, secure transaction protocols, data privacy, and security controls. The evaluation may also consider guidelines related to transaction monitoring, reporting of suspicious activities, and establishing incident response mechanisms. Additionally, the research investigates the enforcement mechanisms associated with these regulations. It assesses the compliance rates among mobile banking service providers, identifies any gaps or challenges in implementation, and explores the effectiveness of audits conducted by regulatory bodies. Furthermore, the collaboration between regulatory authorities, law enforcement agencies, and other stakeholders is a crucial aspect. The research explores the coordination and information-sharing practices between these entities to combat financial fraud effectively. Understanding the level of cooperation and synergy among regulators, industry players, and relevant agencies helps identify areas for improvement and potential strategies to enhance fraud prevention efforts. To gather insights for this aim, the research involves reviewing legal documents, conducting interviews with regulatory authorities and industry experts, analyzing audit reports, and benchmarking against international best practices. By investigating the impact of regulatory frameworks on mitigating mobile banking fraud, the research provides valuable recommendations for strengthening the existing regulations and fostering a more secure mobile banking ecosystem in Bangladesh.

Overall, pursuing these aims contributes to a comprehensive understanding of the effectiveness of advanced technological measures and regulatory frameworks in reducing financial fraud in Bangladesh's mobile banking sector. The findings can inform policymakers, regulators, and mobile banking service providers about the most effective strategies to adopt, resulting in enhanced security, increased customer trust, and a decreased incidence of financial fraud.

Hypothesis:

The hypothesis for the research question "What are the most effective strategies for reducing the incidence of financial fraud in Bangladesh, specifically in the context of mobile banking?" proposes that a combination of robust technological measures, comprehensive regulatory frameworks, and targeted user education initiatives will be the most effective strategies for reducing financial fraud in Bangladesh's mobile banking sector. To begin with, implementing advanced technological measures is crucial. This includes deploying strong authentication mechanisms such as biometrics or multi-factor authentication to ensure secure access to mobile banking services. Additionally, utilizing encryption protocols and secure communication channels can safeguard sensitive customer information during transactions, preventing unauthorized access by fraudsters. Furthermore, integrating real-time fraud detection systems powered by artificial intelligence and machine learning algorithms can identify suspicious activities and patterns, enabling prompt action to mitigate potential fraudulent incidents. In parallel, comprehensive regulatory frameworks play a vital role in mitigating financial fraud.

Establishing stringent guidelines and standards for mobile banking service providers, including security protocols, transaction monitoring, and reporting requirements, can create a solid foundation for fraud prevention. Enforcing compliance through regular audits and penalties for non-compliance ensures that service providers are committed to implementing effective anti-fraud measures. Collaboration between regulatory bodies, law enforcement agencies, and industry stakeholders is also essential to share information, coordinate responses, and stay ahead of evolving fraud techniques. Furthermore, targeted user education initiatives are critical to reducing the incidence of financial fraud. Educating mobile banking users about common fraud schemes, safe banking practices, and how to recognize and report suspicious activities empowers them to make informed decisions and protect themselves from falling victim to fraudsters. User awareness campaigns, interactive training programs, and easily accessible resources can enhance user knowledge and foster a culture of vigilance within the mobile banking community. By combining these three pillars, technological advancements, comprehensive regulatory frameworks, and user education, the hypothesis posits that the incidence of financial fraud in Bangladesh's mobile banking sector can be significantly reduced. These strategies address both the technical aspects of security and the human factor involved in fraud prevention. Ultimately, the goal is to create a secure and resilient mobile banking ecosystem in Bangladesh, promoting trust among users and ensuring the integrity of financial transactions.

Literature Review:

Part 1: With the increasing demand and popularity of the mobile banking system in Bangladesh it has become challenging to keep our mobile banking accounts safe from fraud. Around 30 per cent of banks are exposed to extremely high risks of online fraud and security threats, according to a study. Automated Teller Machine (ATM) and plastic card transactions account for 43 per cent of the frauds, the highest, followed by mobile banking at 25 per cent, it said. The study points out that investment in the banking sector in information technology (IT) professional development is not adequate. Around 40 per cent of the surveyed banks believe that they have a considerable risk of information loss at any moment. Banking Analysts say several disasters occurred in the banking sector due to poor security systems [The Financial Express; Wednesday, 12 July 2023]. However, the banking sector has of late stepped up its efforts. But what is required now is that there should be an increase in the IT budget to ensure risk-free transactions in the banks. This poses a significant threat to online digital fraud and may also trigger serious security threats for the online banking sector. Fraud comes in many forms at the bank; it can be internal, which is committed by employees of the bank itself, or external which is committed by clients, persons, or bodies foreign to the bank. It is becoming very tough to maintain everyone’s accounts safe from traps that are created by fraud people. Fraud has become an especially important risk to Facing financial institutes, credit unions, and banks. They are always trying to crack the security of the users. Combating fraud comes with traditional prevention techniques such as PINs, passwords, and identification systems, however, have become inadequate in modern banking systems. Banks faced fraud in several activities, but remote use of credit appears to be the most vulnerable. Money laundering is also a well-known form of fraud, international lute against this activity is conducted by different states to discover and prosecute criminal activities that occur [Chavan J, Internet Banking-Benefits and Challenges in an Emerging Economy. International Journal of Research in Business Management, 1(1), 19-26 (2013)].

ATM skimming is a high-tech crime in which a criminal electronically steals or skims the cardholder's personal financial information during routine ATM transactions. Globally it is a common crime that forces banks to ensure the security of IT and regulators to force banks to focus on it [A. Kumar and G. Gupta [8]]. In Bangladesh, most ATM frauds were allegedly committed in connivance with the insiders in the banks and outsiders. The regulator has failed to ensure a standard security policy for the banks to protect the interest of customers. Many such cases have gone unreported, as there is no mechanism to get information on this type of fraudulence. The fraud has undoubtedly affected the confidence of customers as well as bankers. The Bangladesh Bank (BB) data shows that after the scam-hit news headlines, transactions through ATMs went down by 40 per cent for a certain time. Earlier, a major incident of credit card fraud was discovered in 2012, at the United Commercial Bank Limited (UCBL) with over Taka 100m withdrawn from it illegally. The money was withdrawn over a period of six years (between sometime in 2007-2012) by a gang of high-tech swindlers, using only 21 credit cards. Of the 56 banks operating in the country, 48 relate to the NPS. At present, there are 9.8 million cards that are used in ATMs and point-of-sales centres in the country. In all cases of debit card fraud, it was found that bank employees were involved in those, either directly or indirectly, and they provided the fraudsters with information about clients [The Financial Express; Wednesday, 12 July 2023].

In the meanwhile, the central bank has produced several measures, including the introduction of chip-based cards and a uniform limit per transaction per day for all banks. It has asked banks to issue chip-based debit cards as soon as possible to protect customers from fraud. A few banks have already moved to EMV (Euro-pay, MasterCard, and Visa) chip cards and PIN issuance, but a large number of banks continue to issue magnetic stripe cards vulnerable to fraud. EMV cards and PINs usually protect against both counterfeit(skimming) and lost or stolen card fraud.

Part 2: The attackers are also developing various kinds of algorithms to present the links of the spam emails to users as the real ones. Government officials and private banks authority working hard to protect their consumers' accounts. Many machines learning-based algorithms have been introduced in the last few years to restrict digital banking threats. Machine learning (ML) on the other hand, offers a more advanced and accurate approach to fraud detection by analysing vast amounts of data and identifying patterns that may indicate fraudulent behaviours. Their main goal is to tackle the problem of fraud in banks and its resolution through Spark with SVM techniques. Support Vector Machine (SVM) can help to reduce risk and improve the quality of service extended to customers to succeed in business. Support Vector Machine (SVM) is a supervised machine-learning algorithm, which can be used for both classification and regression s [Daniel et al. 2009, Bemhard et al. 2010]. SVM is immensely powerful for face recognition, fingerprint identification, voice recognition, and similar task. Several bank authorities use supervised learning methods to Support Vector Machines with Spark (SVM-S) to build models representing normal and abnormal behaviour and then use them to evaluate the validity of new transactions. Spark with the SVM method is the best for these kinds of fraud. The results obtained from databases of credit card transactions show that these techniques are effective in the fight against banking fraud in big data. The experiment result from the study shows that SVM-S has better prediction performance than the Back Propagation Networks (BPN). Fraud detection in Internet banking has also been revolutionized using artificial intelligence (AI), as many businesses have incorporated this technology into their fraud analytics and systems as well. Machine Learning (ML) and Artificial Intelligence (AI) quickly analyse substantial amounts of data to detect fraudulent activities, such as unauthorized transactions or suspicious behaviour patterns [2018 IEEE 9TH Annual Information Technology, Electronics and Mobile Communications Conference (IEMCON)].

Several Techniques have been proposed and used by many researchers, for fraud detection, including credit card fraud. Among these data mining techniques, Bayesian networks, Markov chains, neural networks, linear regression, and sequence alignment are the most popular. Big data applications with data mining techniques can play a key role in the fight against these types of fraud. Data mining is a set of techniques for extracting valuable information from enormous amounts of data tools used to assist in decision-making. Due to rapid change and the development of techniques used by fraudsters, data mining tools can no longer analyse abnormal behaviours [DanielSa, Jose-Mar and LCcerda, 2009), and Bayesian networks [Edgar, Freund and Girosi, 2007]. Big data in this context, come with machine-learning techniques for fraud detection in the database, which is best to fight against banking fraud. Big data applications, like Spark, Hadoop, Cassandra, etc. come with effective algorithms to manage structured, unstructured, and semi-structured data [FATF-GAFLORG, 2016].

Selection of Design:

For the study on "Mobile Banking and Financial Fraud in Bangladesh," a mixed methods research design would be the most appropriate approach. This design integrates both qualitative and quantitative research methods to ensure a comprehensive understanding of the phenomenon. Here are the reasons for selecting a mixed methods design:

Comprehensiveness: Mobile banking and financial fraud are complex and multifaceted issues that require a holistic approach. By combining qualitative and quantitative methods, researchers can gather numerical data (quantitative) as well as in-depth insights (qualitative) to capture the various dimensions of the problem. This approach provides a more comprehensive understanding compared to using a single method.

Quantitative Component: The quantitative component of the research can provide statistical data on the prevalence, frequency, and patterns of mobile banking fraud in Bangladesh. Researchers can survey a large sample of mobile banking users to collect data on their experiences, perceptions, and reported incidents of fraud. Analyzing this data can help identify the extent and impact of the problem, such as the frequency of fraud incidents, the financial losses incurred, and the demographic characteristics of victims.

Qualitative Component: The qualitative component of the research can involve interviews, focus groups, or case studies to explore the underlying factors, motivations, and strategies related to mobile banking fraud in Bangladesh. Qualitative methods can uncover contextual factors, social dynamics, and individual experiences that contribute to the occurrence of fraud. Researchers can conduct in-depth interviews with fraud victims, banking officials, law enforcement agencies, and other relevant stakeholders to gain insights into the modus operandi of fraudsters, the vulnerabilities in the system, and the psychological and emotional impacts on victims.

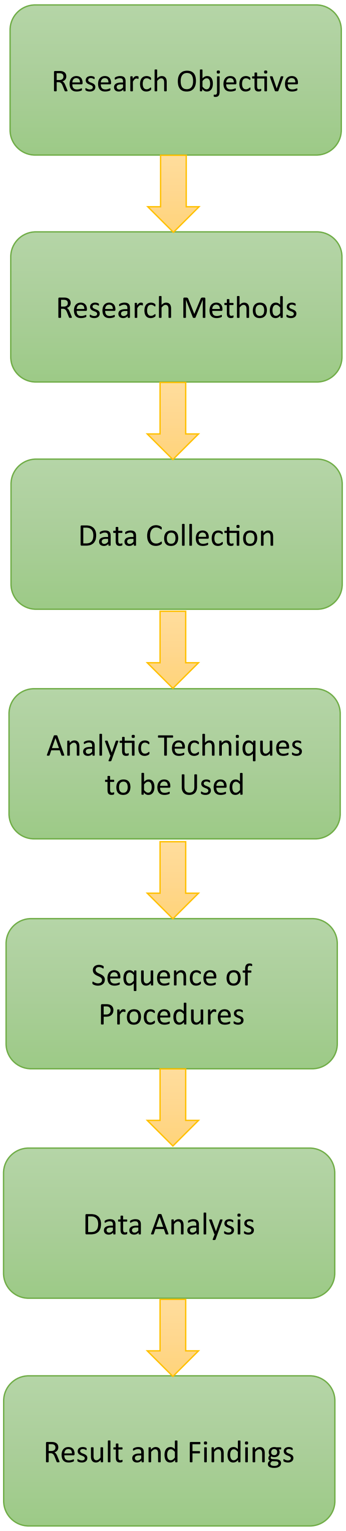
Triangulation: By combining quantitative and qualitative data, researchers can use triangulation to cross-validate findings from different sources. For example, quantitative data on the prevalence of mobile banking fraud can be supplemented and contextualized by qualitative data that sheds light on the underlying reasons behind fraud incidents. Triangulation strengthens the overall validity and reliability of the research, reducing potential biases or limitations of a single method.

Policy and Practical Implications: Mobile banking and financial fraud have significant policy implications for Bangladesh's banking sector and regulatory authorities. A mixed methods design can provide a more robust evidence base to inform policy decisions and the development of effective prevention and intervention strategies. The quantitative data can help quantify the magnitude of the problem and identify key areas of concern, while the qualitative data can provide nuanced insights into the experiences and perspectives of different stakeholders. This combined information can guide the formulation of policies, regulations, and awareness campaigns to mitigate mobile banking fraud and protect consumers.

Sequential or Concurrent Design: In a mixed methods design, researchers can choose either a sequential or concurrent approach. A sequential design involves conducting one phase (qualitative or quantitative) first and using the findings to inform the subsequent phase. A concurrent design involves collecting and analyzing both qualitative and quantitative data simultaneously. The choice between sequential and concurrent design depends on the specific research questions, resources, and time constraints.

In conclusion, a mixed methods research design is well-suited for studying the complex and multifaceted nature of mobile banking and financial fraud in Bangladesh. By integrating quantitative and qualitative methods, researchers can gain a comprehensive understanding of the issue, identify patterns and factors contributing to fraud, and inform the development of appropriate countermeasures. This approach ensures a rigorous and well-rounded investigation into mobile banking and financial fraud in Bangladesh.

Diagram:



Research Variable:

In the research topic of investigating strategies to reduce the incidence of financial fraud in mobile banking in Bangladesh, the following variables can be considered:

Independent Variables:
User Education Programs: The implementation of educational initiatives aimed at raising awareness among mobile banking users about fraud risks, safe practices, and security measures.
Security Measures: The implementation of enhanced security measures such as two-factor authentication, encryption, biometrics, or fraud detection systems by mobile banking providers.

Dependent Variable:
Incidence of Financial Fraud: The occurrence or frequency of fraudulent activities in mobile banking transactions, including unauthorized access, fraudulent fund transfers, identity theft, or phishing attempts.

Scientific Method:

Scientific Method for Investigating Strategies to Reduce Financial Fraud in Mobile Banking in Bangladesh:

Research Question Identification: Clearly define the research question: "What are the most effective strategies for reducing the incidence of financial fraud in Bangladesh, specifically in the context of mobile banking?"

Background Research: Conduct a thorough review of existing literature, studies, and theories related to mobile banking fraud, security measures, and fraud reduction strategies. Gather insights on successful strategies implemented in other countries or contexts.

Hypothesis Formulation: Develop a hypothesis that predicts the relationship between the implementation of specific strategies and the reduction of financial fraud in mobile banking in Bangladesh. For example, "Implementing robust user education and awareness programs, along with enhanced security measures, will lead to a significant decrease in mobile banking fraud incidents."

Experimental Design: Outline the experimental setup, including participant selection or sample size, identification of independent variables and dependent variables. Specify the measurement techniques or instruments to be used.

Data Collection: Conduct the experiment or data collection process, ensuring that it is reliable and valid. This may involve implementing the identified strategies within a specific sample of mobile banking users, tracking and recording fraud incidents, and collecting relevant data on the effectiveness of the implemented strategies.

Data Analysis: Analyze the collected data using appropriate statistical methods or techniques. Employ quantitative analysis to identify patterns, trends, and significant differences in the incidence of mobile banking fraud based on the implemented strategies.

Conclusion Drawing: Evaluate the results in relation to the hypothesis. Determine whether the data supports or refutes the hypothesis and analyze the effectiveness of the implemented strategies in reducing financial fraud in mobile banking in Bangladesh.

Communication of Findings: Prepare a comprehensive research report or presentation to communicate the findings, including the research question, methodology, results, and conclusions. Share the information with the scientific community, policymakers, regulators, mobile banking providers, and other relevant stakeholders. This ensures the dissemination of knowledge and facilitates the implementation of effective strategies to reduce financial fraud in mobile banking in Bangladesh.

<u>Citations:</u>

1. *M. T. Islam and M. A. Tareq, "An impact study on mobile financial services (MFSs) in Bangladesh," Bangladesh Bank, 2018.*
2. *S. Khan, "Combating online frauds and security threats in banks," The Financial Express, February 23, 2016.*
3. *W. Ahmed, "Online frauds and security threats in banks," The Financial Express, July 11, 2023.*
4. *M. Hossain and M. Sulaiman, "A review of Evaluation Metrics for Data Classification Evaluations," International Journal of Data Mining & Knowledge Management Process, vol. 5, pp. 1-11, 2015.*
5. *S. Kovach and W.V. Ruggiero, "Online banking fraud-detection Based on local and global behavior," in Fifth International Conference on Digital Society, Guadeloupe, France, 2011, pp. 166-171.*
6. *IEEE, "Bank Fraud Detection Using Support Vector Machine (SVM)," in 2018 IEEE 9th Annual Information Technology, Electronics, and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada.*
7. *S. Kovach and W. V. Ruggiero, "Online banking fraud detection based on local and global behavior," in Proc. of the Fifth International Conference on Digital Society, Guadeloupe, France, 2011.*
8. *A. Sepehri-Rad, S. Sadjadi, and S. Sadi-Nezhad, "An application of DEMATEL for transaction authentication in online banking," International Journal of Data and Network Science, 2019.*
9. *R. J. Bolton and D. J. Hand, "Unsupervised profiling methods for fraud detection," in Conference on Credit Scoring and Credit Control 7, Edinburgh, UK, Sept 7th, 2001.*
10. *K. N. Karsen and T. G. Killingberg, "Profile based intrusion detection for Internet banking systems," Master Thesis, Norwegian University of Science and Technology, Norway, February 9th, 2008.*