The Implications of Insider Threats in Financial Institutions: A Review of Challenges and Mitigation Strategies

Usman Ibrahim Usman[1]; Muhammad Dini Ibrahim[2]; Ibrahim Abdullahi Aliyu[3]; Umar Isah[4]; Fakhrun Jamal[5]

[1,2,3,4,5]Department of Computer Science and Engineering, Shobhit University, Meerut, Uttar Pradesh, India

Publication Date: 2025/12/10

Abstract: Financial institutions serve as a backbone of our daily life by providing a reliable means to store, transfer and perform online transactions. Insider threat is a great challenge faced by financial institutions, where employees, contractors, or trust partners intentionally or unintentionally misuse or compromise systems that lead to data breaches, unauthorised access and financial loss, and disturbed operations. This paper explores the nature, types, and impacts of insider threats within the financial institutions, outlining both technological and human-related factors. It examines real-world cases of insider breaches, exposing light on the motivations and behaviours behind such incidents. This paper identifies key challenges faced by financial institution, which include difficulties in detection, regulatory burdens, and cultural issues. However, it also highlights numerous mitigation strategies that cover administrative, technical controls, and legal compliance controls (GDPR and HIPAA). The paper also highlights the need for a fair and preventive strategy that integrates technology, awareness, and organisational policy to efficiently handle insider threats in financial institution. It pays particular attention to both technical weaknesses and human factors, such as lack of awareness or personal motivations that lead to unintentional actions. Real-world scenarios are used to illustrate how insider breaches occurred and what kinds of damage they can caused to financial institutions.

Keywords: *Insider Threats, Confidentiality, Integrity, Availability, Financial Institution, Regulatory Compliance.*

How to Cite: Usman Ibrahim Usman; Muhammad Dini Ibrahim; Ibrahim Abdullahi Aliyu; Umar Isah; Fakhrun Jamal (2025) The Implications of Insider Threats in Financial Institutions: A Review of Challenges and Mitigation Strategies.
International Journal of Innovative Science and Research Technology, 10(12), 186-194.
https://doi.org/10.38124/ijisrt/25dec240

I. INTRODUCTION

Insider threat, sometimes known as accidental insider threat, is a component of social engineering. It is important to note that researchers have just recently started to pay more attention to insider threats related to deliberate leaks [1]. “An employee, contractor, or other business partner who has or had authorised access to an organisation's network, system, or data and who purposefully (or inadvertently) exceeds or misuses that access to negatively affect the confidentiality, integrity, or availability of the organisation's information or information systems” is the definition of an insider threat [2].

Organisations throughout the world are still very concerned about the insider threat, and insider threat actors frequently target the financial services sector because it is profitable. Since thieves target valuable assets, banks and financial services organisations are viewed as more appealing targets [3]. Malicious insiders have been a major concern to organisations, particularly financial institutions, as they have greater access to opportunities and resources that could seriously harm the company. Outsiders do not have the same privileges or valid access to facilities and information that insiders do. Insiders also know a lot about the company and its important resources. The insider's extra knowledge makes it easier for them to carry out the attack because they can conceal their hacking operations and trail [4].

Nowadays, insider threats are becoming a very significant or complicated security issue because they can compromise financial institutions' financial assets and sensitive consumer data [5]. Insider threats, whether intentional or unintentional, are always a concern since insiders with privileged cloud access have the ability to cause serious harm in situations where there isn't enough oversight [6].

II. BACKGROUND OF INSIDER THREATS IN FINANCIAL INSTITUTIONS

Insiders are authorised employees who have direct access to resources; in order to gather information or carry out an operation, insiders physically connect to the network and devices. The misuse of confidential data or privileged access is represented by privilege escalation [7]. Insider threats can seriously harm an organisation's financial resources, reputation, and intellectual property [8]. Insider threats are a big problem for the cybersecurity of banks and other financial institutions. They can lead to big data breaches, money losses, and damage to the institution's reputation [9].

An insider who is already a member of an organisation and has authorised access to its resources is the traitor. Workers or subcontractors may pretend to be traitors. Because they already know where the important data is kept, how it is secured, and about any holes that may exist, traitors may steal the information more readily. Furthermore, there is no time limit on preparation or execution because the attack is carried out in accordance with the mission and authority of the person in charge; therefore, adequate time for preparation and attack has already been secured [2]. Unintentional users are those who, occasionally, do acts that endanger the organisation without realising it [10]. People who frequently make mistakes and typically don't give the organisation's security procedures much thought fall into this type of insider. This type of insider unwittingly and unconsciously gives the outside world access to the important resources [11]. [1] claims that unintentional insider threats can come from current or former employees, business partners, and other individuals who accidentally or maliciously grant access to a website or software that uses the network, system, and data of their own company. This can lead to a number of data leaks that harm the interests of the current phase or lower expected income.

Insider threats can seriously harm an organisation's financial resources, reputation, and intellectual property. A number of measures, including employee verification, authentication procedures, training, monitoring, separation of duties, and others, have been put in place by certain firms to reduce insider risks because digital assets are so important and their integrity is crucial to their success. Nonetheless, conventional methods are successful in identifying insider risks and lessening their effects since insiders possess an authorisation trait [12]. Insider threats have the potential to compromise the availability, confidentiality, and integrity of sensitive data, with grave repercussions including industrial espionage, data leaks, and intellectual property theft [13].

III. INSIDER THREATS

A current or former employee, contractor, or business partner who has or had authorised access to an organisation's network, system, or data and purposefully exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organisation's information or information systems is known as an insider threat [12]. Insider threats are malevolent acts committed by partners, contractors, or staff members who have access to a bank's private information and internal systems. Insiders may use their authorised access to steal information, make money, or help outside hackers get into the system. Because insiders may more easily circumvent security measures because these assaults frequently mimic everyday behaviours, they can be challenging to identify [14].

IV. TYPES OF INSIDER THREATS

Insider threats can be classified into several categories depending on or based on the intent and action of the malicious insiders [15]. According to [16], there are three types of insider threats: malicious insiders, negligent insiders, and compromised insiders.

➢ *Malicious Insiders*

Malicious insiders operate intentionally, taking benefit of their facility's privileges to harm the organisation sector. The possible incentives might be financial rewards, a desire to harm the organisation/colleagues, or political/ philosophical beliefs.

➢ *Negligent Insiders*

Negligent insiders are employees who contribute to security breaches by their negligence or ignorance of security measures and policies. These create a great challenge that leads to financial lost, reputational damage and customer trust.

➢ *Compromised Insider:*

A compromised insider is a type of insider threat whereby external parties abuse an insider's credentials or access privileges. They unknowingly facilitate launches brought on by social engineering, phishing, or any other type of compromise.

➢ *Classification of Insider*

Insider risks can be grouped according to their affiliation with the company, as this diagram shows in an organised manner. Insiders are classified into many categories at the highest level according to their affiliation and degree of access. Usually, the pure insider is a direct employee of the company, like a staff worker with permission to access data and systems. Insiders who are not direct employees but have some internal connection, such as contractors or people working in operational jobs like security guards and cleaners, work alongside them. Then there are inside affiliates, who are related to insiders on a personal level. These could be acquaintances, clients, or family members such as a spouse, and they might obtain access indirectly through someone within the organisation. Former employees and outsiders with no direct connection who might work with insiders or make use of insider knowledge fall under the third category, which is known as outside affiliates. When evaluating insider threat threats and creating suitable security responses, it is essential to comprehend the different levels of access and influence that each type of actor may possess, where the classification system aids in the process [4].

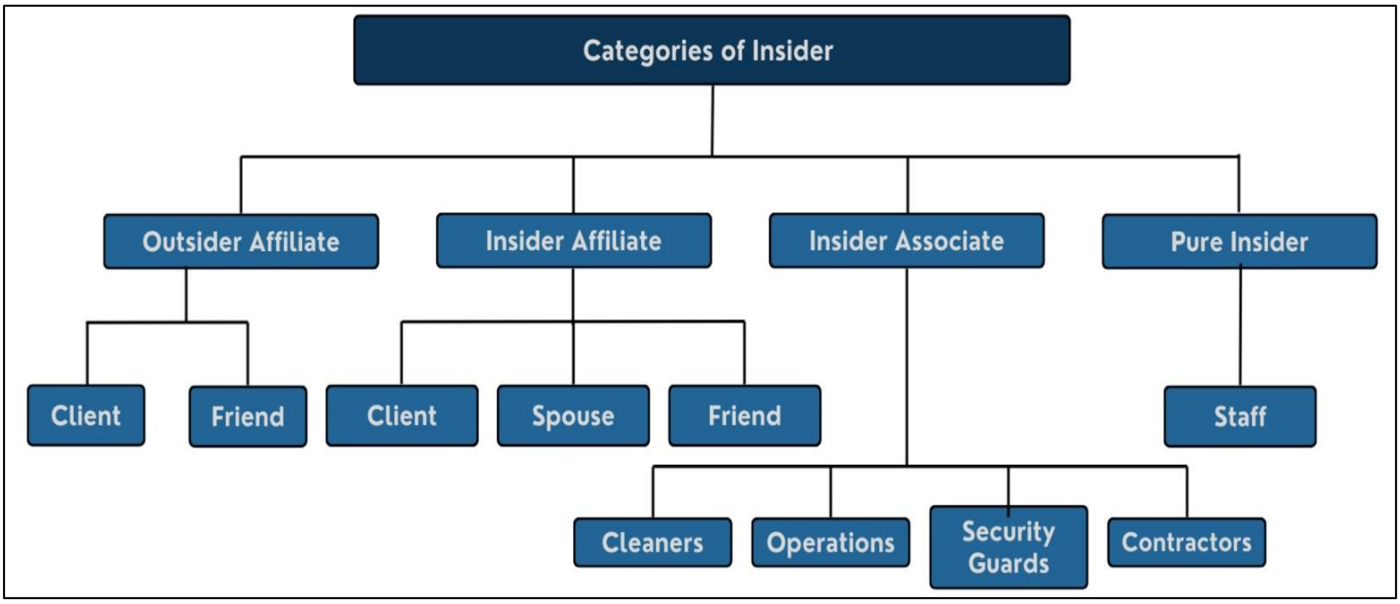

Fig 1 Category of Insider Threats

V. INSIDER THREATS CHALLENGES

Insider threats represent one of the most persistent and damaging forms of cyber risk facing financial institutions worldwide. Unlike external attacks, insider incidents or insider threats arise from individuals or persons with legitimate access to organisational systems; the individuals can be employees, contractors, vendors, or third-party partners who misuse their access unethically [17]. Their thorough understanding or knowledge of financial workflows, authentication procedures, and network structures allows them to bypass many security defences of that organisation [13]. These threats might happen on purpose, leading to data breaches and impersonation using social engineering tricks. To create good preventive and detection measures, you need to know what insiders want and how they act [18].

➢ *Detection Difficulties*

Detecting insider threats that actually misuse network access or access control has particularly become a great challenge in financial institutions, whereby employees have legitimate access to highly sensitive data of that organisation. Malicious insiders can exploit their access by generating network traffic that includes communicating with suspicious external destinations, unauthorised content, and the use of non-standard protocols. Therefore, such misuse of network access can lead to many losses for financial institutions or organisations, including data breaches, financial loss, reputation damage, or regulatory violations. Many insider incidents in financial services involved legitimate user abuse of their access. For instance, an insider threat altered a financial record, installed malicious software, or exfiltrated a customer record [8].

➢ *Human Factors*

The challenges of insider threats are complicated by the multifaceted and dynamic nature of human behaviour [12]. Human factors involve a decision, action, or mistake made by an individual person that can impact the security of a particular organisation. For instance, a receptionist employee who does not realise the security threat to the system can click on the insecure links, which may allow threat outsiders to get access to the system or key resources [10]. Human behaviour or factors are recent challenges in financial intuition, but they can be addressed through a combination of human intervention and technical solutions [8]. Individual and organisational sociotechnical indicators of insider threat risk, as well as other pertinent indicators that can be identified based on personal history elements, are highlighted in research on human behavioural factors supporting the establishment of an ontology [3], [5].

➢ *Cultural and Organizational Issues*

Insider threat has consistently been identified as a key threat in both private and public sector organisations, especially those that are part of the nation's critical infrastructure. To protect critical assets, organisations must recognise the distinctions and breadth of this threat. Sometimes organisations don't have strict rules about using things like USB drives, or they don't really enforce the security policies they do have. In workplaces where there's too much trust and not enough oversight, it becomes easier for insiders, whether by mistake or on purpose, to plug in a USB and end up introducing malware into the system [10].

➢ *Regulatory and Compliance Burdens*

Financial organisations are realising more and more that manual compliance does not guarantee consistent adherence to regulatory requirements, which have been subject to a constant stream of modifications. As a result, financial institutions used regtech solutions, which offer a productive way to deal with these expenses [19]. In the financial sector, following local, national, and international regulations is an important but difficult undertaking. Detailed paperwork must be sent to the appropriate authorities, large data sets must be analysed, and many factors must be reviewed [20].

- *Weak Governance and Oversight Structures*

One of the most prominent or significant challenges facing financial institutions both in Nigerian and global contexts is the absence of strong governance and standard frameworks dedicated to insider risk management. In recent years, Nigeria's financial sector has transitioned into a digital ecosystem, which has led to tremendous innovation and progress as well as exposure to increasingly complex cyberthreats. Nigeria currently values protecting its financial institutions because its economic development heavily depends on digital financial services. In many Nigerian banks or financial institutions, insider threat management is integrated within general cybersecurity policy, without a difference based on structure for monitoring privileged accounts or behavioural anomalies. Lack of separation of duties and poor audit trail management create opportunities for internal abuse [21]. Moreover, the major system security breaches persist mostly in smaller financial institutions, especially those with limited or no investment in Security Operation Centres (SOCs) and advanced security practice. The absence of SOCs contributes to reactive rather than proactive responses to internal incidents. The U.S. CERT Insider Threat Centre emphasises that governance deficiencies significantly increase the mean time to detect (MTTD) insider threat within an organisation, which tends extending beyond 200 days of breaches [22].

- *Insider-Outsider Collusion*

The insider-outsider collusion, which involves staff members (insiders) of an organisation grouping together with cybercriminals (outsiders) to enable fraudulent activities or reveal private information to the cybercriminals for financial gain. Economic pressures, job insecurity, and weak ethical culture contribute to employee lack of trust. Globally, collusion is becoming more complex threat vector. Financial institution across the globe faces challenges involving instances of employees being recruited via social media or bribed by organised cybercrime groups to reveal organization financial and customer information for financial gain [22]. Threat attribution is made more difficult by these hybrid attacks, which make it difficult to differentiate between internal and external attack vectors.

- *Employee Privilege Misuse and Credential Exploitation*

In financial institution, privilege misuse occurs when individual/employee with higher levels of system privilege access, including IT administrators or finance officers, utilise their credentials to change records, access private information, or carry out fake transactions. Weak access control and failure to swiftly remove credentials following changes in employee position or resignations from financial institution increase the danger in many fintech companies, especially in developing nations [18]. Insider threats linked to privilege abuse often occur from excessive access rights or poor monitoring of employee activities, which allow malicious attackers to operate undetected within the systems. Equally concerns is the issue of credential exploitation, where attackers gain access through compromised or shared accounts due to weak credentials or social engineering attacks techniques. Employees negligence may unintentionally expose credentials by reusing passwords or storing them insecurely, providing an entry point for external cybercriminals. To mitigate these risks, organisations most implement optimise principle of least privilege, conduct continuous access audits, and employ behavioural analytics to detect anomalous user activity [20].

- *Inadequate Insider Awareness and Behavioural Monitoring*

Lack of investment in employee awareness regularly and behavioural monitoring programmes by numerous financial institutions pose a greater setback in minimising insider threats. Studies show that most Nigerian banks conduct cybersecurity training only during the onboarding process, with limited reinforcement thereafter [23]. Employees often remain unaware of subtle indicators of insider manipulation or social engineering techniques. Organisations face challenges in balancing employee monitoring with privacy and labour laws. Regulations such as the EU's General Data Protection Regulation (GDPR) restrict intrusive behavioural surveillance, limiting the effectiveness of some insider detection programs [17]. Furthermore, employee behavioural analytics systems require substantial data to train anomaly detection models, yet insider incidents are statistically rare and create huge data imbalance gaps [21].

- *Whistleblower Fear and Ethical Constraints*

The psychological and organisational barriers to whistleblowing techniques constitute a major drawback to early insider threat detection mechanisms. In Nigeria, despite the presence of whistleblower provisions in the Central Bank of Nigeria's Code of Conduct, cultural aversion to "betraying colleagues" remains strong [21]. Whistleblowers are afraid of retaliation or loss of trust by co-workers, hindering them from reporting suspicious activities within the financial institutions. In global contexts, despite the existence of whistleblower programs, challenges persist in ensuring anonymity and preventing victimisation. Many institutions lack mechanisms to integrate whistleblower inputs into incident response workflows [17].

- *Inadequate Forensic and Incident Response Capabilities*

Cybersecurity incident response and forensic readiness capacity remains weak in many developing countries. In Nigerian context, financial institutions often depend on outsourcing external digital forensics expert, leading to inconsistent response times and evidence contamination [22]. The absence of specialised insider threat analysts further limits incident containment and root-cause analysis, although large multinational banks maintain robust SOCs but tend to struggle with cross-departmental coordination, particularly between cybersecurity, HR, and compliance teams during the investigation process [18]. Insider threats can be mitigated through prevention of data breaches, protection of intellectual property, compliance requirements, improved cybersecurity posture, and behavioural analysis and training.

VI. INSIDER THREATS MITIGATION STRATEGIES

Mitigating insider threats requires a multidisciplinary and multilayered approach that integrates technological tools, human resource management, and ethical governance to convert an insider in a financial institution. Numerous institutions have invested in and adopted multiple techniques to prevent their organisation and resources from insider threat attacks.

- *Strengthening Governance and Oversight*

Financial institutions must establish Insider Threat Governance Units (ITGUs) by integrating cybersecurity, frameworks, human resources, and regulatory compliance. These units should enforce and monitor privileged accounts, conduct regular access reviews, and enforce least-privilege principles [17]. In Nigeria, regulatory enforcement by the CBN and NFIU requires quarterly insider risk audits from financial institutions; moreover, in a global context, institutions can adopt the Insider Threat Program Maturity Model (ITPMM) developed by Carnegie Mellon University to benchmark progress [21].

- *Advanced Detection and Analytics*

With the current advancement in emerging technologies, intelligence threat detection and analytics models were developed, including User and Entity Behaviour Analytics (UEBA), Data Loss Prevention (DLP) tools, and Security Information and Event Management (SIEM) systems. These technologies analyse behavioural baselines and detect deviations indicative of insider activity [18]. In Nigeria, cost constraints limit adoption; however, cloud-based UEBA solutions can reduce infrastructure overhead. Globally, AI and federated learning approaches have improved anomaly detection while preserving employee privacy [19].

- *Access Control and Credential Hygiene*

Implementing Zero Trust Architecture (ZTA) principles ensures that no internal user is automatically trusted. Continuous authentication, micro-segmentation, and strict privilege management can reduce misuse risk [20]. Financial institutions should enforce immediate de-provisioning of user credentials upon exit and employ Privileged Access Management (PAM) solutions to monitor administrative actions [21].

- *Awareness, Ethics, and Training*

Sustainable mitigation requires changing employee behaviour. Regular, scenario-based training using real cases of insider fraud within local contexts enhances risk perception [22]. Nigerian banks, for example, can develop multilingual awareness modules (Hausa, Yoruba, Igbo) to broaden understanding.

Globally, organisations should embed ethical decision-making frameworks into employee evaluations and promote a “See Something, Say Something” culture without fear of retaliation [23].

- *Whistleblower Protection and Ethical Reporting*

Encouraging early reporting through anonymous digital whistleblowing platforms and reward systems fosters transparency [24]. The Nigerian government’s 2016 Whistleblower Policy demonstrated that financial incentives significantly increased disclosures of misconduct. Financial institutions should build on this success by guaranteeing confidentiality and integrating whistleblower data into insider threat dashboards [25].

- *Incident Response and Forensic Readiness*

Developing in-house digital forensics capabilities is critical. Financial institutions should train analysts in evidence handling, log correlation, and behavioural investigation. Establishing national Insider Threat Response Centres under entities like NFIU or CBN could centralise expertise and coordination [21]. Globally, organisations are adopting post-incident learning frameworks, combining forensic evidence with behavioural analysis to prevent recurrence [17], [22].

- *Integrative Strategy*

Ultimately, an effective insider threat mitigation strategy must be holistic, addressing not only technology but also human psychology and governance culture. For Nigeria, emphasis should fall on ethical transformation, localised awareness, and regulatory enforcement, while globally, continuous analytics and AI-driven behavioural modelling represent the frontier of proactive insider threat defence.

- *Technical Measures*

The concept of confidentiality, integrity, and availability, which is the CIA model, in addition to authentication, is ensured to protect sensitive data of an organisation, including financial institutions or organisations. Unauthorised access can be used by a malicious insider to leak sensitive information, misuse resources, or change information integrity. Malicious insiders are able to access organisational resources, learn about key organisational assets, and win the organisation's trust [7]. Financial organisations can implement Zero Trust Architecture (ZTA), Multi-Factor Authentication (MFA), and access control models like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), which are vital in minimising unauthorised access as technical measures [24].

- *Administrative/Organizational Measures*

Insiders will take advantage of any holes in the organisation's policies to harm it; thus, it is crucial to make sure the policies are clear, succinct, and focused on the rationale behind them. Furthermore, these policies may cause inner dissatisfaction and encourage hostile actions if they are misinterpreted or not regularly accepted. Organisations frequently distribute copies of these rules to all staff members, who then sign them. At the organizational level, the law entails preventing data exfiltration techniques, implementing explicit security policies for staff members at all organizational levels, enforcing consistent, stringent access controls and monitoring procedures for privileged users, and penalising rule violations [11].

- *Behavioural and Psychological Monitoring*

Mitigating insider threats requires an understanding of the human elements that affect cybersecurity, with particular attention to the critical roles that individual differences, organisational culture, and human behaviours play [13]. According to [8], behavioural and psychological monitoring is described as a process or method of observing insiders with privileged access who may intentionally or inadvertently compromise security through malicious actions or negligent behaviours, which can be achieved by implementing least privilege principles, monitoring and auditing activities, conducting regular training for employees and awareness training, implementing access control, and finally establishing transparency and accountability.

➢ *Legal and Regulatory Approaches*

In response to the global implementation of stricter data protection regulations, such as the updated General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), some financial organisations or bodies have adopted zero-trust architectures, which by default prevent data disclosure unless access is specifically authorised. Furthermore, financial institutions must constantly calculate their liquidity coverage ratios and net stable funding ratios in order to comply with Basel III's strict liquidity standards [25].

- *Insider Threat Risk Assessment and Mitigation Cycle*

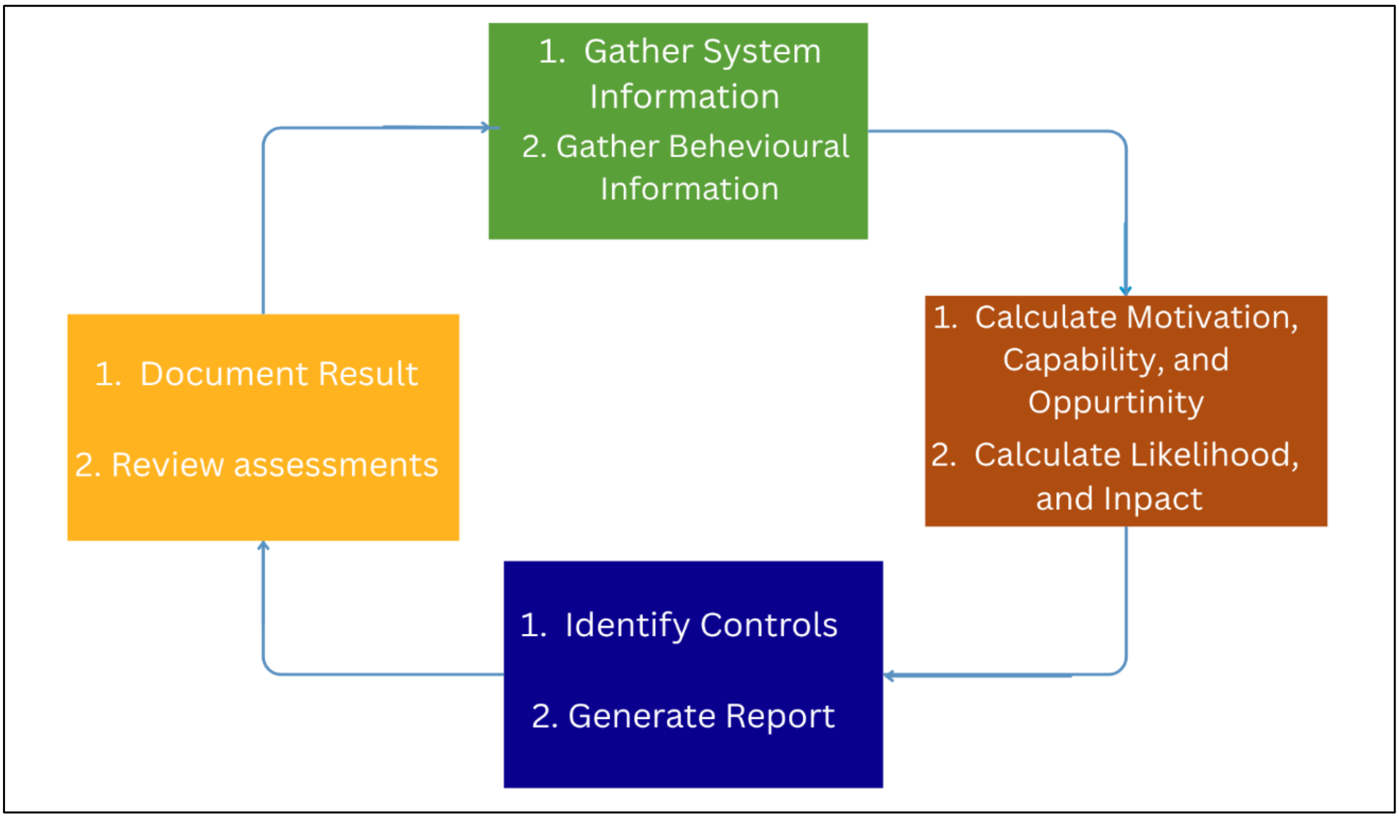
1. Gather System Information
2. Gather Beheavioural Information
1. Calculate Motivation, Capability, and Oppurtinity
2. Calculate Likelihood, and Inpact
1. Identify Controls
2. Generate Report
1. Document Result
2. Review assessments

Fig 2 Insider Threat Risk Assessment and Mitigation Cycle

The cyclical procedure, or method, for evaluating and reducing insider threats within an organisation, which can actually cause damage, is shown in the diagram above. In order to establish a baseline understanding of user activities and the environment in which they operate in the sector; it initially starts with gathering information and behavioural and system-related data. After that, important risk factors are assessed, including the person's motive, opportunity, and capacity to do a dangerous act, as well as the possible chances of the event occurring together with their consequences. The results of this risk assessment are briefly summarised in a comprehensive report together with the identification of appropriate/suitable controls. In order to ensure that knowledge is recorded and advancements may be achieved, the procedure proceeds with a comprehensive review of the evaluation and documenting of the outcomes. This feeds back into the cycle, encouraging continuous observation and improvement of the strategy for detecting and preventing insider threats [5].

VII. CASE STUDIES OR REAL-WORLD EXAMPLES

At this particular stage, the literature review that was conducted will highlight some real-world examples and case studies that happen or occur in financial institutions by insider threats.

A. Insider Threats in Nigerian Financial Sector

Insider threat has been recognised as a critical security problem globally, especially within the financial sector, as the Nigeria Deposit Insurance Corporation (NDIC), a self-governing corporation responsible for regulating the banking industry in Nigeria and helping the Central Bank of Nigeria (CBN) to promote a safe and sound banking system in Nigeria, noted insider fraud perpetrated by bank staff, often in collusion with external actors, has been responsible for a significant proportion of fraud cases [26], [27].

➢ *Case 1: The 2014 Cyber Heist*

- Insider Profile: An IT worker of the bank
- Incident Detail: In a publicly reported event in 2014, a Nigerian bank that was ISO27001 compliant, a recognised standard for Information Security Management Systems (ISMS), and adhering to the Central Bank of Nigeria guidelines, reported a cyberattack that resulted in a financial loss to the tune of £23.5 million. The attack was carried out by an IT worker of the bank collaborating with an outsider. This incident reveals that despite compliance with laid standards on security, organisational security is highly dependent on users [28].

➢ *Case 2: Modern Insider Threat (2022–2024)*

- Incident Detail: A report [21], recently conducted, reveals that insider threat attacks on Nigerian financial institutions rose by 92% from 2020 to 2024. The report also reported that Distributed Denial of Service (DDOS) attack have a response time typically within two hours of the attack, while insider threats detection/response time extended to 120 hours, highlighting the difficulty institutions face in recognizing and mitigating internal security breaches in comparison to external attacks. It further revealed that a major insider threats resulted in $500,000 fraud case over the period, out of 9330 fraud cases studied, 40% of the attacks were supported by insiders. In another report that studied selected banks, the report [26] revealed that 30% of the reported fraud incidents are insider-related, dominating other fraud types like unauthorised transfers.

B. *Insider Threats in Indian Banking System*

➢ *Case 1: Shamrao Vithal Cooperative (SVC) Bank Data Leak (2019)*

- Incident Detail: In 2019, SVC filed a First Incident Report (FIR) with the police following a breach of trust and data leakage that resulted in a loss of approximately Rs 29 crore. The case was filed against two current employees and a former employee that was general secretary of the employees' union prior to being fired in 2017 for misbehaviour. The investigation of the case revealed that 447 confidential customer records were illegally accessed and shared outside the bank server. The FIR was filled under several sections, including Section 408 for criminal breach of trust by a clerk or servant, Section 109 for punishment for abetment, the Information Technology Act (IT Act) 2000, Section 43A for compensation for failure to protect data and Section 66 for computer-related offences, among other Indian Penal Code [29].

➢ *Case 2: Uttar Pradesh Cooperative Bank (UPCB) Attempted Withdrawal*

- Incident Detail: A former UPCB bank manager was arrested by the Uttar Pradesh Police following an illicit withdrawal of Rs 146 Crore, equivalent to 16.3 million dollars. The former manager was arrested alongside an accomplice when they visited the bank building and attempted to hack the bank server directly from the server room of the bank. Following the visit, two attempts were made to withdraw the money from the bank official account, but the bank was able to detect the transactions and blocked them. An FIR was filed with the police following the incident, and 10 other staffers of the bank were suspended because of lapses by the bank [29], [33].

C. *Historical Incidents*

Irrespective of whether malicious actions by insiders were deliberate or accidental, they can create an equally negative effect, such as stealing, leaking and damaging confidential data, or even assisting external attackers by building backdoors for them to attack. The seriousness of attacks initiated by insiders can be observed from the subsequent examples of actual real-world incidents (historical cases). The initial example, a severe insider attack that damaged the image of both the Federal Bureau of Investigation (FBI) and the U.S., was done by a staff member of the U.S. National Security who leaked very confidential data to Russian agencies. A further insider attack incident was executed by a soldier of the U.S. Army who leaked large, highly classified government documents to WikiLeaks. Additionally, the most serious fraud occurrence, which cost the Societe Generale French bank an estimated sum of $7 billion, was committed by one of its employees [17]. An estimated $10 million was lost by Bank of America as a result of an insider attack in which a bank employee gave criminals access to hundreds of client records [3]. A Capital One employee was found accountable in 2020 for a data breach that exposed transaction records and personal information about millions of customers [14].

➢ *Authentication Helps Lessons Learnt.*

The most crucial aspect of detecting insiders is figuring out their purpose. Motivation can be classified as personal, financial, revenge, and political [7]. Financial issues, like health issues or family problems, can influence or motivate an insider to steal the organisation's information for monetary benefit. Human behaviour, technological flaws, and organisational failures are only a few of the causes of insider threats. These risks have the potential to have disastrous outcomes, including serious financial losses and harm to one's reputation [13].

➢ *Future Direction*

Looking ahead, insider threats in financial institutions are likely to become more complex and harder to detect. As banks and other financial organisations rely more on cloud services, artificial intelligence, and remote work arrangements, employees and contractors will have new ways to access and move sensitive data. Attackers may exploit advanced tools, such as AI-driven phishing or deepfake technology, to trick insiders into sharing information or granting access.

Another concern is the growing use of third-party vendors and partners. While they help institutions run more efficiently, they also create more entry points for potential misuse of access rights. The blending of personal and professional devices, especially in remote work setups, will continue to blur security boundaries, making it easier for mistakes or malicious actions to slip past monitoring systems. In the future, the line between intentional and unintentional insider actions may be even harder to draw. This means financial institutions will need to adapt quickly, using smarter detection tools, stronger identity verification, and ongoing awareness programmes to keep up with the changing risk landscape.

VIII. RECOMMENDATIONS

➢ *Improve Staff Awareness*

Regular training should be conducted for all employees to help them understand how insider threats work and how to avoid risky actions which may lead to data loss. People are less likely to make mistakes when they know what to look out for.

➢ *Use Strong Technical Controls*

Organisations have to make a system that has features of security guards, like Zero Trust, access control models (RBAC and ABAC), and multi-factor authentication (MFA) should be in place to limit access of the users or employees. These systems can help prevent both intentional and accidental (unintentional) insider attacks.

➢ *Monitor Behaviour and Access Patterns*

Financial institutions or organisations should be tracking how their employees interact with systems. Unexpected changes in behaviour or access patterns could signal a potential threat.

➢ *Review and Enforce Policies*

Organisations have to have clear rules and regulations about data handling, USB use, system access, and information sharing that must be enforced or implemented. Policies should always be reviewed frequently and updated when needed.

➢ *Legal and Compliance Checks*

Institutions must stay up to date with legal rules such as GDPR, HIPAA, and PCI-DSS. Meeting those legal standards helps avoid fines and improves overall data protection.

➢ *Encourage a Culture of Security*

Creating a workplace or interface where security is everyone's responsibility makes it harder for insider threats to succeed. This includes open communication, trust with verification (zero trust policy), and regular security audits.

IX. CONCLUSION

Insider threats are rapidly growing most especially in the financial institutions. These threats come from people who already have access to sensitive systems or data, and those people are employees, contractors, or business partners of that particular organisation. The review has shown that insider threats can happen for many reasons; some people may act intentionally or unintentionally (whereby others may do so by mistake or because they were deceived), These threats can damage an organisation's finances, reputation, and customer trust. Financial institutions face many challenges in dealing with insider threats. These include the difficulty in detecting or identifying insider actions, the complexity of human behaviour, weak organisational policies, and the heavy burden of following legal and compliance rules. Real-world incidents or case studies show that even one insider can cause serious damage or harm to an organisation.

To reduce or mitigate some of the risks, financial institutions must take action on multiple levels. Technical solutions like Zero Trust Architecture, access controls, and multi-factor Authentication helps stop unauthorised access, but technology alone is not enough. Organisations should also train their staff by inviting a cybersecurity expert, and making sure policies are clear and implemented. Regular monitoring and understanding human behaviour are also key parts of reducing insider threats.

REFERENCES

[1]. L. Xiangyu, L. Qiuyang, and S. Chandel, "Social Engineering and Insider Threats," in 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Nanjing: IEEE, Oct. 2017, pp. 25–34. doi: 10.1109/CyberC.2017.91.

[2]. A. Kim, J. Oh, J. Ryu, and K. Lee, "A Review of Insider Threat Detection Approaches With IoT Perspective," IEEE Access, vol. 8, pp. 78847–78867, 2020, doi: 10.1109/ACCESS.2020.2990195.

[3]. F. Whitelaw, J. Riley, and N. Elmrabit, "A Review of the Insider Threat, a Practitioner Perspective Within the U.K. Financial Services," IEEE Access, vol. 12, pp. 34752–34768, 2024, doi: 10.1109/ACCESS.2024.3373265.

[4]. M. N. A. Mhiqani et al., "A new taxonomy of insider threats: an initial step in understanding authorised attack," Int. J. Inf. Syst. Manag., vol. 1, no. 4, p. 343, 2018, doi: 10.1504/IJISAM.2018.094777.

[5]. G. Kul and S. Upadhyaya, "Towards a Cyber Ontology for Insider Threats in the Financial Sector".

[6]. T. J. Olorunlana, "Securing the Global Cloud: Addressing Data Sovereignty, Cross-Border Compliance, and Emerging Threats in a Decentralized World," Int. J. Sci. Archit. Technol. Environ., pp. 1394–1407, May 2025, doi: 10.63680/ijsate0525102.117.

[7]. A. Subhani, I. A. Khan, and A. Zubair, "Review of insider and insider threat detection in the organizations," J. Adv. Res. Soc. Sci. Humanit., vol. 6, no. 4, Dec. 2021, doi: 10.26500/JARSSH-06-2021-0402.

[8]. M. N. Al-Mhiqani et al., "A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations," Appl. Sci., vol. 10, no. 15, p. 5208, July 2020, doi: 10.3390/app10155208.

[9]. D. Alexander and S. Kenneth, “ML-Based Anomaly Detection for Insider Threats in Financial Institutions,” vol. 16, no. 01, 2025.

[10]. U. Inayat, M. Farzan, S. Mahmood, M. F. Zia, S. Hussain, and F. Pallonetto, “Insider threat mitigation: Systematic literature review,” Ain Shams Eng. J., vol. 15, no. 12, p. 103068, Dec. 2024, doi: 10.1016/j.asej.2024.103068.

[11]. N. Saxena, E. Hayes, E. Bertino, P. Ojo, K.-K. R. Choo, and P. Burnap, “Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses,” Electronics, vol. 9, no. 9, p. 1460, Sept. 2020, doi: 10.3390/electronics9091460.

[12]. T. Al-Shehari and R. A. Alsowail, “An Insider Data Leakage Detection Using One-Hot Encoding, Synthetic Minority Oversampling and Machine Learning Techniques,” Entropy, vol. 23, no. 10, p. 1258, Sept. 2021, doi: 10.3390/e23101258.

[13]. N. F. M. Nassir, U. F. A. Rauf, Z. Zainol, and K. A. Ghani, “REVEALING THE MULTI-PERSPECTIVE FACTORS BEHIND INSIDER THREATS IN CYBERSECURITY,” vol. 17, 2024.

[14]. F. Jimmy, “Cybersecurity Threats and Vulnerabilities in Online Banking Systems,” Int. J. Sci. Res. Manag. IJSRM, vol. 12, no. 10, pp. 1631–1646, Oct. 2024, doi: 10.18535/ijsrm/v12i10.ec10.

[15]. N. Ayanbode, O. A. Abieba, N. Chukwurah, O. O. Ajayi, and A. I. Daraojimba, “Human Factors in Fintech Cybersecurity: Addressing Insider Threats and Behavioral Risks,” Int. J. Multidiscip. Res. Growth Eval., vol. 5, no. 1, pp. 1350–1356, 2024, doi: 10.54660/.IJMRGE.2024.5.1.1350-1356.

[16]. USA and A. Gunuganti, “Insider Threat Detection and Mitigation,” J. Math. Comput. Appl., pp. 1–6, Aug. 2024, doi: 10.47363/JMCA/2024(3)184.

[17]. R. A. Alsowail and T. Al-Shehari, “Techniques and countermeasures for preventing insider threats,” PeerJ Comput. Sci., vol. 8, p. e938, Apr. 2022, doi: 10.7717/peerj-cs.938.

[18]. N. Ayanbode, O. A. Abieba, N. Chukwurah, O. O. Ajayi, and A. I. Daraojimba, “Human Factors in Fintech Cybersecurity: Addressing Insider Threats and Behavioral Risks,” Int. J. Multidiscip. Res. Growth Eval., vol. 5, no. 1, pp. 1350–1356, 2024, doi: 10.54660/.IJMRGE.2024.5.1.1350-1356.

[19]. A. A. Papantoniou, “Regtech: steering the regulatory spaceship in the right direction?,” J. Bank. Financ. Technol., vol. 6, no. 1, pp. 1–16, June 2022, doi: 10.1007/s42786-022-00038-9.

[20]. A. Srivastava, B. Pandiya, and N. S. Nautiyal, “Application of Artificial Intelligence in Risk Assessment and Mitigation in Banks,” in Artificial Intelligence for Risk Mitigation in the Financial Industry, 1st ed., A. K. Mishra, S. Anand, N. C. Debnath, P. Pokhariyal, and A. Patel, Eds., Wiley, 2024, pp. 27–52. doi: 10.1002/9781394175574.ch2.

[21]. C. I. Ezekwe, “INTERNATIONAL JOURNAL OF RESEARCH AND INNOVATION IN SOCIAL SCIENCE (IJRISS),” SSRN Electron. J., 2025, doi: 10.2139/ssrn.5065151.

[22]. O. Efijemue, I. Ejimofor, and O. S. Owolabi, “Insider Threat Prevention in the US Banking System,” Int. J. Soft Comput., vol. 14, no. 3, pp. 17–28, Aug. 2023, doi: 10.5121/ijsc.2023.14302.

[23]. Akintayo Micheal Ajayi, Abraham Okandeji Omokanye, Olawale Olowu, Ademilola Olowofela Adeleye, Olayinka Mary Omole, and Ifeoluwa Uchechukwu Wada, “Detecting insider threats in banking using AI-driven anomaly detection with a data science approach to cybersecurity,” World J. Adv. Res. Rev., vol. 24, no. 2, pp. 123–132, Nov. 2024, doi: 10.30574/wjarr.2024.24.2.3182.

[24]. D. Almaiah, “Journal of Cyber Security and Risk Auditing Vol.2025, No.4”.

[25]. P. Radanliev, “Digital security by design,” Secur. J., vol. 37, no. 4, pp. 1640–1679, Dec. 2024, doi: 10.1057/s41284-024-00435-3.

[26]. B. U. Umoh, U. D. Ofurum, and O.-A. S. Folasade, “The Impact of Bank Fraud on Economic Stability and Public Trust in Nigeria’s Financial System,” vol. 6, 2024.

[27]. E. G. Kasie and N. C. Emeka, “NIGERIA DEPOSIT INSURANCE CORPORATION AS A PANACEA FOR STABILIZING NIGERIA BANKING INDUSTRY,” vol. 1, no. 2, 2024.

[28]. T. H. Fagade and T. Tryfonas, “Security by Compliance? A Study of Insider Threat Implications for Nigerian Banks: HCI International 2016,” Hum. Asp. Inf. Secur. Priv. Trust, pp. 128–139, June 2016, doi: 10.1007/978-3-319-39381-0_12.

[29]. G. Dahiya, “Insider Led Cyber Fraud in Indian Banking System,” vol. 11, no. 6, 2022.

[30]. Uchenna Joseph Umoga, Enoch Oluwademilade Sodiya, Olukunle Oladipupo Amoo, and Akoh Atadoga, “A critical review of emerging cybersecurity threats in financial technologies,” Int. J. Sci. Res. Arch., vol. 11, no. 1, pp. 1810–1817, Feb. 2024, doi: 10.30574/ijsra.2024.11.1.0284.

[31]. C. I. Ezekwe, “Analysis of Emerging Cybersecurity Threats in Nigeria’s Financial Sector: Trends, Impacts, and Mitigation Strategies,” Int. J. Res. Innov. Soc. Sci. IJRISS, 2025, doi: 10.2139/ssrn.5065151.

[32]. A. Chakraborty, “Cyber Security Threats In Indian Banking Sector And Implementation Of AI As A Preventive Measure,” vol. 14, no. 4, 2024.

[33]. “Retired manager of UP Cooperative Bank under lens for online attempt to siphon off ₹146 cr,” Hindustan Times. Oct. 2022. Accessed: Oct. 30, 2025. [Online]. Available: https://www.hindustantimes.com/cities/others/retired-manager-of-up-cooperative-bank-under-lens-for-online-attempt-to-siphon-off-rs-146-cr-101666109923029.html