Advances in Artificial Intelligence and Machine Learning; Research 5 (2) 4004-4033 Received 7-03-2025; Accepted 21-06-2025; Published 28-06-2025

Mitigating Cyberfraud in Financial Institutions: A Deep Learning Approach using the South African Banking Industry as a Case Study

Oluwatoyin Esther Akinbowale Oluwatee01@gmail.com
Faculty of Economics and Finance,
Tshwane University of Technology (TUT), South Africa

Mulatu Fekadu Zerihun ZerihunMF@tut.ac.za
Faculty of Economics and Finance,
Tshwane University of Technology (TUT), South Africa

Polly Mashigo MashigoMP@tut.ac.za
Faculty of Economics and Finance,
Tshwane University of Technology (TUT), South Africa

Corresponding Author: Oluwatoyin Esther Akinbowale

Abstract

Cyberfraud is a major threat to the banking and financial institutions globally and South Africa is not an exemption. The deep learning (DL) technique for cyberfraud incidence classification and time series prediction using the South African financial institutions as a case study was demonstrated in this study. Secondary data from the South African Banking Risk Information Centre (SABRIC) was employed and the data was trained under the DL paradigms of Convolutional Neural Network (CNN) and the Long Short-Term Memory (LSTM) model. For both models, the adaptive moment estimation (ADAM) algorithm was employed for fraud incidence classification while the time series model was used for the future prediction of fraud incidences. On the overall, the LSTM model with an accuracy of 96.80% outperformed the CNN model with an overall accuracy of 96.17%. Moreover, the accuracy, precision, recall and F1-score of the LSTM classification model namely 72.14%, 87.43% and 77.31% respectively exceeded 70%. The results show that the DL model can be deployed for fraud classification and time series analysis of fraud incidences. The outcome of this study may promote cyber resilience and sustain the fight against the perpetration of cyber-related fraud in the South Africa. The use of the CNN and LSTM models for cyberfraud classification and time series prediction of cyberfraud incidences demonstrated in this study is unique. This study contributes conceptually, theoretically and empirical to knowledge on cyberfraud mitigation. It proposes an artificial intelligence based conceptual framework for reinforcing cybersecurity in the financial institution.

Keywords: Artificial intelligence, Cyberfraud, Deep learning, Financial institutions, Incidence classification

Citation: Oluwatoyin Esther Akinbowale, et al. Mitigating Cyberfraud in Financial Institutions: A Deep Learning Approach using the South African Banking Industry as a Case Study. Advances in Artificial Intelligence and Machine Learning. 2025;5(2):226.

1. INTRODUCTION

Cyberfraud is a major threat to the banking and financial institutions globally. The evolution of digital technologies which led to the proliferation of digital banking products and services has radically transformed the banking operations but with increased vulnerabilities to cyberattacks [1, 2]. It has enabled the financial institutions to expand their digital products and services with improvement in the efficiency of delivery [3, 4]. It also promotes financial inclusion through ease of access to banking products and services especially in remote and rural places [5]. However, the deployment of digital technologies for banking operations has been identified as one of the root causes of cyberfraud perpetration resulting in significant financial loss, loss of goodwill and reputation amongst others [6–9]. Threat actors are becoming more sophisticated in their operations and exploiting individual's and organisation's vulnerabilities to launch cyberattacks in the forms of phishing, social engineering, malware, identity theft, and intrusions to commit fraud. The reports of the South African Banking Risk Information Centre (SABRIC)[10], indicates that digital fraud continues to increase in scope and scale in terms of the magnitude of incidences reported and gross amount lost despite the efforts of the financial institutions geared towards cyber resilience.

The South Africa Reserve Bank (SARB) coordinates and regulates the operations of banks and financial institutions in South Africa to ensure uniformity, robustness and safety of operation [11]. Despite the efforts of the SARB and other stakeholders, the rate of cyberfraud perpetration in South Africa is still high due to non-implementation of policy, legal and regulatory framework coupled with shortage of cybercrime experts as well as technological sustainable solutions geared towards cyberfraud detection and prevention.

INTERPOL [12], reported that in South Africa, the perpetration of crypto currency fraud resulted in the loss of $588 million and $3.6 billion in Bitcoin in 2020 and 2021 respectively. Cryptocurrency fraud is one of the emerging digital frauds in South Africa which may take the form of fake digital trading or investment platforms.

Kaspersky's report [13], reported that the African is one of the most targeted continents in 2023 by the cyber criminals while Surfshark's report [14], indicated that South Africa is the leading country in the African continent and placed fifth in the world in terms of cybercrime density Therefore, the rate and magnitude of cyberfraud perpetration in South Africa put the country on a global spotlight and that is why the financial institutions are used as a case study in this study.

In 2018, a total of 23,466 digital banking fraud incidents were reported across the digital banking channels resulting in a gross loss of R262,826,888 while in 2019 the total number of reported cases increased by 20% with 8% increase in the gross loss compared to 2018 [15, 16]. In 2020 and 2021, there was a reduction in the number of digital banking fraud by 18%, however, the gross losses from the sum of R310,484,349 in 2020 to R438,238,743 in 2021 accounting for 41.14% increase. In 2022, there was an increase of 24% in digital banking fraud compared 2021 with 68% increase in gross losses (from R440,123,125 in 2021 to R740,847,488 in 2022 mostly due to social engineering). In 2023, digital banking fraud incidence increased by 45% compared to 2022 with 47% increase in gross losses compared to 20222. This increase was attributed to surge in banking applications fraud, which accounted for 60% of the total digital banking fraud cases as well as other fraud techniques such as social engineering [10, 16–19].

TABLE 1 summarises some statistics on cyberfraud incidences in as reported by SABRIC.

Table 1: Cyberfraud incidences in South Africa from 2018-2023

Nature of cyberfraud	Year	Reported cases	% difference in reported cases	Gross loss (Rands)	% difference in gross loss
Banking applications	2018	7,465	–	104,883,325	–
	2019	10,668	43	108,389,041	3.34
	2020	10,281	−3.63	123,990,231	14
	2021	12,254	19.19	219,248,397	55.5
	2022	16,639	35.78	363,322,114	50
	2023	31,612	89.99	625,712,552	74
Online banking	2018	3,915	–	129,002,523	–
	2019	3,304	−15.60	171,705,112	33.10
	2020	3,943	19.34	139,786,621	−20
	2021	5,866	48.77	198,055,406.25	35
	2022	9,455	61.18	348,198,319.36	55
	2023	11,068	17.06	411,706,461	2
Mobile banking	2018	11,826	–	28,941,040	–
	2019	12,575	6.33	28,245,948	−2.40
	2020	21,083	73.61	45,786,257	47.38
	2021	11,040	−47.64	17,529,549.72	−89.25
	2022	10,077	−8.72	29,633,899.52	51.32
	2023	9,904	−1.75	44,974,096	43
Card not present (Debit and	2018	–	–	890,300,000	–
credit card) Account take	2019	–	–	1,007,000,000	20.5
over, card not present, false	2020	–	–	993,547,709	−1.34
application and counterfeit	2021	–	–	1,163,476,761	17.1
(On South African issued	2022	11,110	–	959,435,838	−17.54
card across all countries)	2023	39,251	253.294	1,126,348,584	17.4

Source: SABRIC report [15–19]

From TABLE 1, it can be deduced that individuals and financial institutions in South Africa are still faced with the challenge of cyberfraud perpetration.

[8], identifies lack of effective supervision and control as some of the reasons for cyberfraud perpetration while [6], queried the efficacy of the anti-fraud technologies deployed in mitigating cyberfraud.

Several efforts have been made to mitigate cyberfraud in South Africa. For instance, cybercrimes law (Cybercrimes Act 19 of 2020) have been enacted and passed into law in 2022 [20]. The law plainly defines cybercrime and classifies the offences that constitute cybercrimes. This law serves as a deterrent measure and also aid the investigation as well as prosecution processes of the threat actors. South Africa also embrace a multidisciplinary approach involving the synergy of relevant institutions have been deployed. Some of the synergy include the partnership of the South

African Police Service (SAPS) with the Council for Scientific and Industrial Research (CSIR) to establish a ”Cybercrime Designated Point of Contact” to provide the SAPS with access to some CSIR’s expertise such as forensic analysis and cybersecurity and enhance its capacity to efficiently investigate cybercrime in a time effective manner [21]. Similarly, a collaborative platform known as the “Fusion Centre” has also been established by the Financial Intelligence Centre (FIC). The platform brings together the law enforcement, investigative bodies intelligence, and criminal justice bodies to facilitates the timely sharing of intelligence reports and financial intelligence in order to prevent financial crimes and aid effective cyberfraud investigation [22].

The conventional method of cyberfraud detection which is rule-based is useful, but may not adequately adapt to the dynamics of threat actors and the evolving cyberfraud risks. This necessitates the application of the DL approach which is a subset of Artificial Intelligence (AI) that models intricate trends in datasets to classify and predict cyberfraud occurrences. This method continues to gain traction due to its potential to accurately classify and predict cyberfraud incidence thus, assisting the relevant stakeholders in cyberfraud mitigation to make informed decisions. Unlike other machine learning techniques, the DL algorithms such as CNN and LSTM employed in this study can learn and model financial dataset to detect trends and anomalies and to make predictions. The deployment of this AI-based innovative solution can ease the burden on the financial institutions and regulatory bodies with an improved fraud prevention and detection systems which can make the fight against cyberfraud more effective and sustainable. Thus, this study explores the application of DL techniques in the prediction and classification of cyberfraud using the dataset obtained by SABRIC from 2018-2023. This study is important in that it may aid the fight against cyberfraud via intrusions detection and real time forecast of the trends of cyberfraud incidences and their associated losses over time. Furthermore, it may also assist in the investigation of the effect cyberfraud perpetration by visualising the losses incurred by financial institutions over a period. It contributes to knowledge by leveraging on the potentials of DL thereby providing a more proactive, data-driven and intelligent fraud mitigation approach that can promote cyber resilience in the financial institutions. This study offers technological solutions driven by AI for cyberfraud classification and prediction. The classification of cyberfraud will aid ease of visualisation to understand the trends, the impact of the existing mitigation approach as well as the number of occurrences and corresponding gross losses so that the right policy and steps can be undertaken to mitigate other vulnerabilities exploited by the threat actors. Although South Africa was used as a case study in this study, nevertheless, the conceptual framework developed in this study and the procedural steps for applying the DL model for cyberfraud mitigation is not limited to the South Africa context. Other countries could also adopt or modify the models to combat cyberfraud.

The structuring of this work is done as follows: the review of the existing literature is highlighted in section 2 while section 3 details on the methodology employed (DL approach). Section 4 discusses the results obtained followed by some policy implications. This study ends with conclusion, recommendations and directions for future work.

2. LITERATURE REVIEW

2.1 Overview of Cyberfraud Perpetration and Detection Approaches

Cyberfraud is a digital crime involving intrusion into individuals or organisation's sensitive information or organisation's account to commit fraud. It also encompass other forms of unathorised transactions carried out online primary to defraud information or organisation. Cyberfraud perpetration in the financial institution represents a major global challenge resulting in loss of money and reputational damage [23–25] with South Africa experiencing a growing trend in digital financial crime [10, 16, 17, 26] indicated that the threat actors primarily target are the Internet of Things (IoT) devices which enable connection with Internet and facilitate exchange of data with other systems or devices communications networks. Perpetrators also employs various forms of social engineering such as phishing, malware, vishing etc. to gain unauthorized access in individual's or corporate accounts to commit fraud. Recently crptocurrency fraud has also emerged whereby threat actors deceive victims to invest in fake investment or trading platforms for the primary purpose of siphoning invested funds. The growing rate of cyberfraud perpetration has been linked to the increase in the number of Internet users, recent advances in technology resulting in the digitalisation of financial and banking services, adoption of remote operations and exploitation of the vulnerabilities of individuals and financial institutions [6, 27–33]. The rule based system or statistical approaches employed for cyberfraud detection is limited due to their inability to adapt to the evolving cyber threats and dynamic behaviours of the threat actors [34]. Studies have indicated the potentials of AI for fraud mitigation, leveraging on its ability to learn, adapt and predict possible changes over time [35]. However, machine learning models may also be limited in the areas of feature extraction, trend detection, identification of complex and non-linear which are necessary in fraud detection. Thus, the exploration of the DL such as CNN, and LSTM has the potential to overcome this challenge due to their ability to learn and extract hierarchical features from raw data and capture the temporal dependencies in financial transaction data which is necessary for fraud detection and mitigation [36].

Literature further show that DL models have improved fraud detection process compared to the traditional classifiers especially in the detection of anomalies or fraud patterns in card transactions [37]. Iscan and Akbulut [38], demonstrated the use of the LSTM for detecting fraudulent transaction in e-wallet transactions while Aros *et al.* [39], reported on financial fraud detection using machine learning based models to detect anomalies in financial transaction dataset especially credit card and insurance frauds and the outcome of the study indicated that the developed models are accurate in detecting anomalies while recommending the use of DL and reinforcement learning techniques in financial fraud detection.

2.2 The South African Context

The digital banking system was introduced to South African banking around 1996, and has led to the radical transformation of the sector in terms of operational excellence, financial inclusion, speed and effectively delivery banking product and services [40]. However, the proliferation of cyberthreats also increased with the digitalisation of the banking services leaving the financial institutions with cyberfraud risk to contend with. The continuous increase in cyberfraud incidences have resulted

in financial and non-financial losses to the financial institutions [41–45]. South Africa tops the list of African countries with the highest rate of cybercrime and ranked fifth globally in terms of cybercrime density [14]. The cyberfraud perpetration impacts individuals, organisation and the economy at large. For instance, Moatshe [46], reported that annual cost of cybercrime in South Africa has risen to R2.2 billion. This has significant implication on the economy

The annual reports of SABRIC from 2018 to 2024 grouped digital fraud into three major categories namely banking application fraud, online fraud and mobile application fraud and the major techniques employed by the threat actors to carry out these frauds is via social engineering in the forms of phishing, smishing, vishing, email hacking, spamming, sim swap and business email compromise etc. Studies attributed increase in cyberfraud in South Africa to data exposure or breaches [47],less stringent or non-enforcement of cyberlaws [45] as well as loopholes in cyber-defence or organisation's controls [6, 7].

Although some efforts have been made to mitigate the occurrence and impact of cyberfraud in South Africa, however, the impact is still significant in terms of financial losses, damage to reputation, data exposure and compromise amongst others [9, 48] Some efforts aimed at mitigating cyberfraud in South Africa include legislation and improvement and implementation of regulatory and policy frameworks. For instance, the new cyber law highlights the activities that constitute cybercrime and empowers the police in the investigative role [20]. Furthermore, Section 6(5) of the Bank Act 94 of 1990 specifies alignment of the South African banks to cyber risk management measures to prevent cyber attack, and promote effective response cyber disruptions [49]. In terms of regulatory framework, majority of the banks in the sub-Sahara Africa including South Africa have adopted the "BASEL" regulatory framework to minimise financial risks and ensure cyber resilience and operational safety [50–55].

Existing literature advocates for the development and implementation of cyber risk management framework as a counter measure to the growing cyber risk [6, 56] while some authors suggested synergy among the security stakeholders, increase in public sensitization and cybersecurity awareness, effective implementation of cyber laws, training and human capacity development in the areas of cybersecurity and deployment of anti-fraud technologies, effective authentication systems and internal controls, amongst others [6, 7, 19, 57–60].

2.3 Theoretical Literature Review

Two theories were adopted in this study to establish the integration of AI-based models for real time classification and prediction of cyberfraud trends. These are the Technology Acceptance Model (TAM) and Anomaly Detection Theory (ADT). TAM was developed by Davis [61], and describes how users accept and adopt a technology based on two premises: perceived usefulness (which determines the extent to which the stakeholders such as the bank professionals believe that DL model assist in fraud classification and detection), and perceived ease of use (which relates to the extent to which the DL models are perceived as users friendly and could easily be integrated into the existing detection systems).

This theory underscores the need for organisational readiness and support in deploying AI-based models for cyberfraud detection. The perception of users is important in the integration of the

proposed method because AI-models are generally perceived as disruptive models which requires certain changes to be made in the existing security architecture of the organisation to integrate the AI models. Secondly, the practical feasibility of deploying AI-based model for fraud classification and detection must be ascertained. In this regard, other issues such as the privacy and ethical issues must be addressed. AI-based models thrive on big data, thus, the capacity for the acquisition of large volume of dataset in real time in a transparent manner must also be ascertained.

The second theory; ADT perceives cyberfraud as an ”anomaly” within the context of a normal transaction. The theories emphasise the use of detection mechanisms to identify outliers, irregular behaviours and trends within a normal pattern. Thus, it aligns with the use of the DL models—especially the LSTM and CNN models for anomaly detection. In the context of cybrfraud, the anomaly represents the fraud that should be detected within a normal transaction. DL models has the capacity to learn, identify complex and non-linear relationships within a dataset, adapt, extract important feature, classify patterns, detect trends detection, and make projections [62]. Hence, the features of the DL models justifies its use for classifying and detecting fraud in line with the ADT.

2.4 Empirical Literature Review

The literature reports on the use of single DL model and hybrid learning models for intrusion detection. The use of single DL model has been demonstrated by Chandran *et al.* [63], who employed the deep belief network (DBF) for malware detection and classification. The results obtained indicated that the proposed model has F1 score of 97.33%, precision of 97.42%, and recall of 97.33% which indicates the suitability of the DL model for intrusion detection and classification. Also, Shende and throat [64], employed the LSTM model to detect cyberattack using the KDD99 dataset. The binary classification gave an accuracy of 99.2% accuracy while 96.9% accuracy was obtained for the multiclass classification. Furthermore, the work of Jony and Arnob [65], involving the LSTM model using the CIC-IoT2023 dataset gave an accuracy of 98.75% and F1 score of 98.59%. In addition, the use of the feed-forward neural network for features extraction in Windows application by Saxe and Berlin [66], gave an accuracy of 95% with a false positive rate of 0.1% [66].

Other efforts geared towards intrusion detection in IoT devices using integrated DL models have been reported in the literature. For instance, TABLE 2 presents the overview of the hybrid approaches employed for intrusion detection including the methodology employed for intrusion detection and the results obtained and the implications.

The outcome of the empirical review indicates that hybrid DL outperforms the single DL model and the conventional machine learning model due to the ability of one model to compensate for the weaknesses of the other. By leveraging on the strengths of both models, intrusions can be detected with high accuracy within a limited time before it escalates into fraud.

Table 2: Overview of existing hybrid approaches employed for intrusion detection

Authors	Method	Outcome	Implications
Awad *et al.* [67]	Integrated Improved Long Short-Term Memory (ILSTM), Chaotic Butterfly Optimization Algorithm (CBOA) and Particle Swarm Optimization (PSO). The NSL-KDD dataset and LITNET2020 datasets were employed for binary and multi-class classifications to detect intrusions.	The integrated ILSTM-CBOA-PSO has of 93.09% accuracy and of precision 96.86% compared to the ordinary LSTM with 82.74% accuracy and 76.49% precision.	This implies that AI-based hybrid forms models can detect intrusions better than the ordinary models
Ibitoye *et al.* [68]	Machine learning based approach featuring the Feedforward Neural Network (FFN) and the Self-normalizing Neural Network (SNN). The BoT-IoT dataset was employed for intrusion detection	FNN performed better than the SNN for intrusion detection with an accuracy of 95.1% However, the accuracy of FFN reduced to 24%, 18%, and 31% respectively when three adversarial samples were introduced while the SNN model showed better stability and resilience adversarial samples.	This indicates that the machine learning model is also suitable for intrusion detection although there might be some trade-offs such as accuracy of detection, stability and resilience to intrusions during the selection of the algorithm
Abbas *et al.* [26]	DL models such as Deep Neural Network (DNN), CNN and RNN were employed.	The first variant of the RNN outperform other models with 96.61% accuracy, 98.55 % precision and F1-score of 98.57%	The results validate the suitability of the RNN DL model for intrusion detection in IoT devices.
Dhanya *et al.* [69]	Combines machine and deep learning for intrusion detection.	The decision tree model produced the highest classification accuracy of 99.05% compared to the ensemble technique but the lowest detection of 99% for reconnaissance attacks while the Random Forest model produced the second best classification with an accuracy of Random (98.96%) and the highest detection accuracy of 99%.	The outcome validates the stance that an integrated machine and deep learning approach is suitable for detection of intrusion or network attack.

Table 2: Continued..

Authors	Method	Outcome	Implications
Kolosnjaji *et al.* [70]	Combines CNN and RNN for hierarchical feature extraction, as well as the N-gram technique for detecting malware	The result gave 89% detection accuracy.	Performance evaluation indicates that the combined approach outperform other existing approaches deployed for similar task.
Rhode *et al.* [71]	Ensembles Recurrent Neural Networks (RNNs) for malware detection	The result gave an accuracy of 94% within 5 s and 96% within 10 sec while single RNN gave an accuracy of 89%	The accuracy increases with increase in detection time and the number of networks. The study demonstrate the possibility of balancing accurate detection of intrusion with time effectiveness. This implies that intrusions can be detected and blocked before it escalates into fraud using the proposed approach.
HaddadPajouh *et al.* [72]	Recurrent Neural Networks (RNNs) DL model with different LSTM configurations for malware detection	The result gave the highest detection accuracy of 98.18% for 2-layer neuron configuration.	This implies that RNNs are suitable for intrusion detection
Halbouni *et al.* [73]	Integrated CNN-LSTM	The CNN-LSTM model with 3-layers gave the highest accuracy followed by the 3-layer LSTM-CNN model and 2-layer CNN-LSTM model	The high accuracy of the integrated model was linked to the CNN's ability to extract spatial features and the extraction of temporal features by the LSTM model.
Hnamte and Hussain [74]	Integrated CNN-biLSTM	The outcome of the multiclass classification gave a 100% and 99.64% accuracy rate for two datasets respectively	The integrated approach leverages on the strength of each model to detect hidden pattern or latent intrusions thus, outperforming the machine learning approaches or single DL approaches

Table 2: Continued..

Qazi *et al.* [75]	Integrated CNN–RNN approach	The proposed approach gave an accuracy of 98.90% which was higher than the conventional machine learning model	The high accuracy was linked to the capability of the CNN to collect features and the ability of the RNN too extract the collected features
Lan *et al.* [76]	Hybrid CNN architecture	The proposed method gave high F1 score and stability thereby indicating that the integrated model is robust for the designated task	The hybrid model demonstrates the capacity of identifying normal access to network and intrusions

2.5 Research Gap

The literature reviewed underscores the need to investigate the application of DL models for cyberfraud classification and detection. This is due to the fact that research on application of DL models for the classification and detection of cyberfraud detection is limited. For instance many existing works in South Africa focused on the use of quantitative or qualitative approach for the investigation or mitigating cybercrime, as well as conceptual and systematic review of cybercrime in the banking sector [6, 9, 47, 77]. Furthermore, the exploration of DL models such as CNN, RNN and LSTM application with the capacity to classify cyberfraud and project the impact in terms of financial losses have not been widely reported in the literature. This leaves a gap in the deployment of AI-driven solutions to cyberfraud classification and detection. The exploration of these research gaps explored in this study will aid the understanding of the progress made regarding cyberfraud mitigation and also assist the stakeholders in effective planning and decision making in real time.

3. METHODOLOGY

FIGURE 1, presents the techniques employed in this study. Secondary data from SABRIC was employed and the data was trained under the DL paradigms of CNN and LSTM models. For both models, the ADAM algorithm was employed for training the dataset for the fraud incidence classification assignment while the time series model was used to predict fraud incidences.

3.1 Overview of Dataset

Datasets from the SABRIC reports [10, 15–19] were employed in this study. It consists of four major classes of digital crime prevalent in the South African financial institutions categorized as banking applications, online banking, mobile banking and card fraud (TABLE 1). The datasets provided

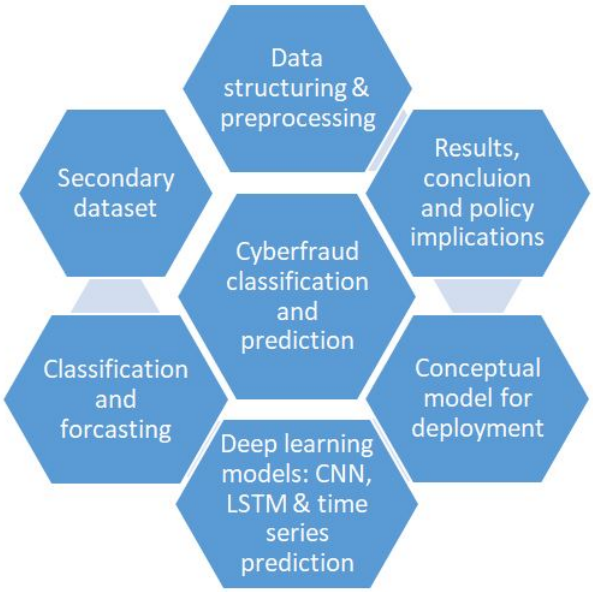

Figure 1: The overview of the method employed

information about the nature of cyberfraud perpetrated, reported cases, gross loss and differences in gross loss from 2018-2023. The first category of fraud is the banking application fraud. This encompasses all fraud incidences perpetrated via bank apps such as intrusion into accounts by threat actors using stolen or compromised log in, token or authentication details etc. Online banking fraud involves the transfer of funds online or other forms of illegal transactions perpetrated online while Mobile banking fraud involves the use of social engineering such as phishing, vishing or SIM swap by fraudsters intrude into personal mobile banking account for fraud perpetration [16].

FIGURES 2 and FIGURES 3, present the reported cyberfraud incidences and their corresponding gross losses from 2018 to 2024 as reported by SABRIC [10, 15–19]. This dataset was employed for classification using the CNN and LSTM model as well, time series analysis and prediction.

3.2 The CNN Architecture

Cyberfraud incidents are characterised by sequence of operations such as theft of confidential information, social engineering etc. thus, the choice of the CNN model stems from the fact that it is suitable for extracting spatial features and capturing local dependencies [73, 75] as well as identifying the relationships within sequence of operations that depicts fraud. FIGURE 4, presents the architecture for the CNN. The dataset was formatted and arranged in a matrix form as follows:

```
Xcell N x 1 cell array of [features x time steps] matrices
YN x 1 categorical vector
```

Figure 2: Reported cases of cyberfraud in South Africa (2018-2023)
Source: Authors (Raw data extracted from SABRIC reports, 2018-2023).

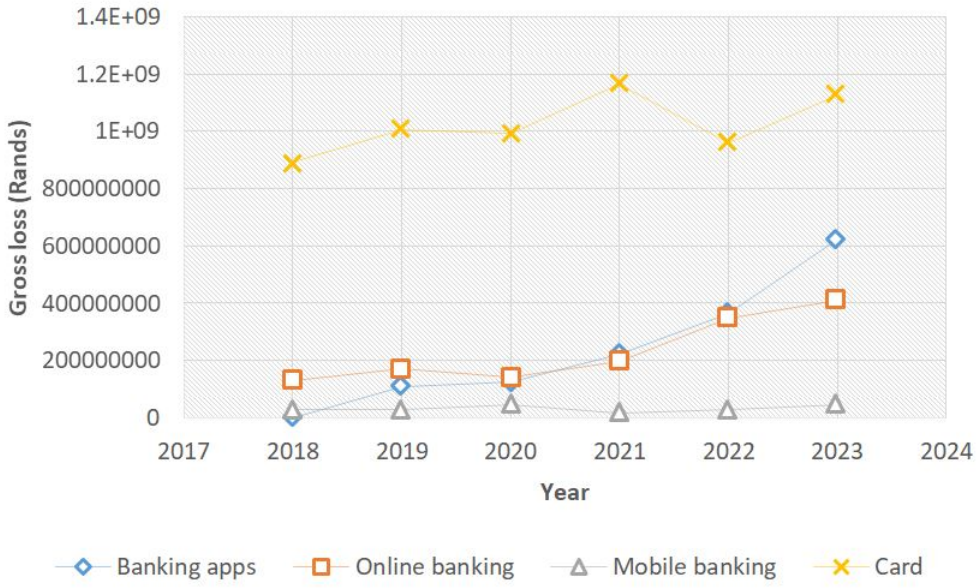

Figure 3: The gross loss due to cyberfraud (2018-2023)
Source: Authors (Raw data extracted from SABRIC reports, 2018-2023).

Each block comprises of 6 rows (from 2018 to 2023) and each row has 4 values (representing reported cases, percentage difference in reported cases, ross loss n Rands and percentage difference in gross loss. Thus, the Timesteps (T) = 6, Features (F) = 4 and Samples (N) = 4. The datastet is

preprocessed by cleaning it and replacing missing values (-) with 0 and thereafter stored in a 3D array as required by CNN input.

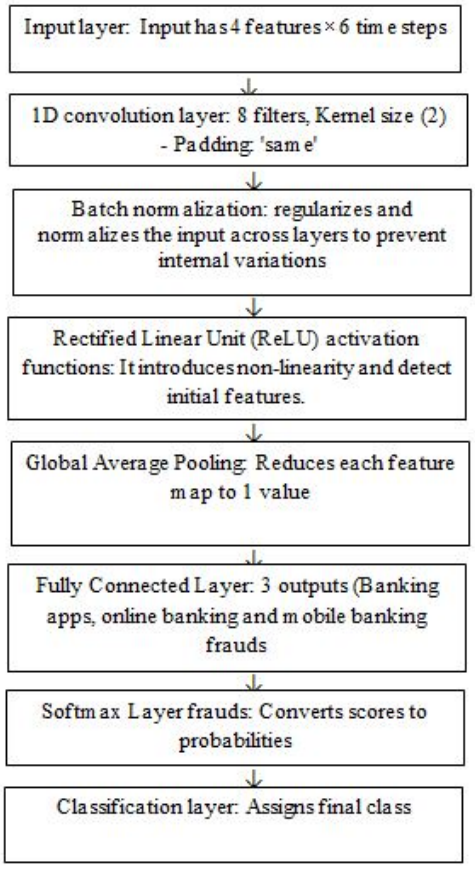

Figure 4: The architecture for the CNN

3.3 The LSTM Architecture

The LSTM is form of recurrent deep neural network suitable for extracting temporal features [69, 73]. Hence, it can be used for the analysis of historical information of time series data such as cyberfraud dataset employed in this study and for long-term nonlinear series prediction. The LSTM was employed in this study for classifying cyberfraud. Like CNN, it can capture complex trends, and process sequences of data with short or long-term dependencies or relationships [65, 78]. In the context of cyberattack, the LSTM model can detect the details of communication, network traffic or intrusions to aid the risk mitigation plans. FIGURE 5, shows the LSTM architecture at time step t comprises of four gates namely "input gate" (i) and "output gate "o" as well as "forget gate" (f) and "cell candidate gate" (g). Information is taken in at the input gate (i) where decision is also taken and the information added or stored in the cell state where it is updated accordingly. The "forget gate" (f) takes decision on the information to be deleted from the cell state while the output gate (o) regulates the amount of information added to the cell state and provides the output.

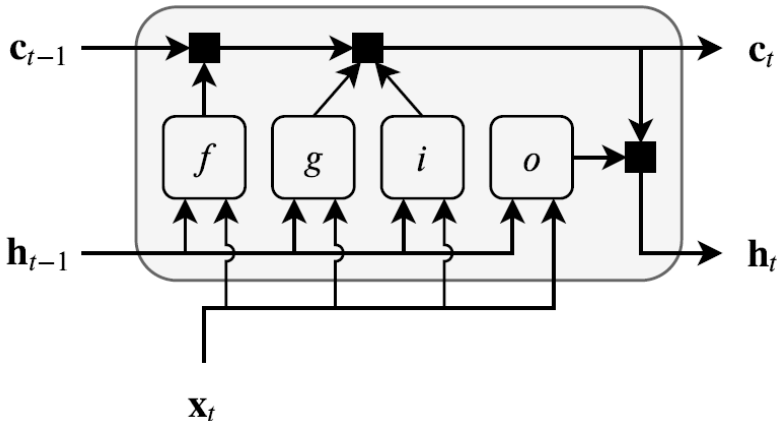

Figure 5: The LSTM architecture

The LSTM layer weight comprise of the following: input weights denoted as W, the recurrent weights represented by R, and the bias denoted as b. Equation 1 shows the chains of the weights W, R, and b respectively.

$$W = \begin{Bmatrix} W_i \\ W_f \\ W_g \\ W_o \end{Bmatrix}' \quad R = \begin{Bmatrix} R_i \\ R_f \\ R_g \\ R_o \end{Bmatrix}' \quad b = \begin{Bmatrix} b_i \\ b_f \\ b_g \\ b_o \end{Bmatrix}' \tag{1}$$

FIGURE 6, presents the architecture of the LSTM model comprising of five layers namely input, LSTM, fully connected, Softmax and output layers. The LSTM layer has 32 hidden unit with output mode 'last'. It processes the temporal fraud incidence sequence and encodes temporal dependencies. The `'last'` mode outputs the hidden state at the final time step, which depicts the summary of the sequence of events.

The implementation of the CNN and LSTM models for cyberfraud incidence classifications was done in the MATLAB 2022b environment. The network was trained to identify and classify frauds occurrence into three major categories namely: banking application, online banking and mobile banking using features extracted from the dataset.

TABLE 3, presents the parameters for the CNNLSTM model.

The performance evaluation of the CNN and LSTM models was calculated using evaluation criteria presented in equations 2-5.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}} \tag{2}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{3}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{4}$$

$$\text{F1score} = 2 \cdot \frac{\text{Precison} * \text{Recall}}{\text{Precison} + \text{Recal}} \tag{5}$$

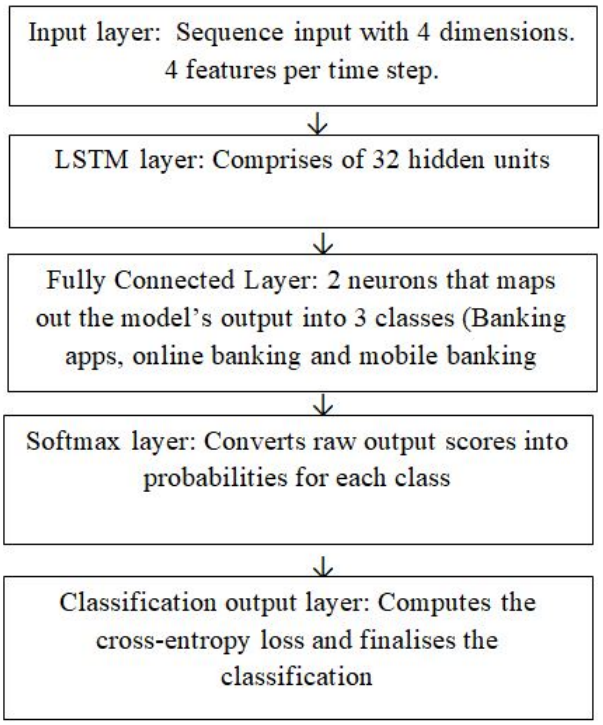

Figure 6: The architecture for the LSTM

Table 3: The LSTM model parameters.

Parameter	CNN	LSTM
Optimizer/ algorithm	ADAM	ADAM
Rate of Learning	0.001	0.001
LSTM 1 hidden nodes	-	200
LSTM 2 hidden nodes	-	100
Epoch/Iteration	50/200	100/400
Elapsed time	3 mins 2 sec	1 min 21 sec
L2regularization (weight decay) to prevent overfitting	0.0001	0.0001
Loss function for multi-classification	Cross entropy	Cross entropy
activation function	ReLU	Gate (Sigmoid) and state(tanh)
Gradient threshold	1	1

3.4 Forecasting Time Series Data using LSTM

The future time steps forecasting was conducted by training the LSTM model in a sequence-to-sequence manner, having the training sequences as the responses adjusted by one time step. This is to predict the succeeding time step for each of the input sequence, and update the state of the network according after each prediction.

The LSTM model can capture both short and long term dependencies, thus employed for predicting the severity of the cyberfraud incidences using normalized values from 0-1 using historical dataset on percentage of gross loss. The dataset is arranged as a single time series, with time steps that corresponds to the gross loss and corresponding year of occurrence which. The data is prepared as a row vector with the output comprising of a cell array, in which each of the elements is a single time step and scaled for enable effective training process.

One of the significance of this LSTM model is that it can updated in real time as new data arrives or as new values are obtained. The model is reset to make new predictions so as to prevent past predictions from influencing the outcome of the new predictions.

4. RESULTS AND DISCUSSION

4.1 Multi Classification of Cyberfraud Incidences using the CNN Model

FIGURE 7, shows the progress of the training of the CNN model for 200 iterations. The iteration terminated at 50 epochs after the convergence of the solution without over fitting. The accuracy plot expressed in percentage indicates that the accuracy of the model increases from initial value of 0% to over 80% as the number of iterations increases which indicates that the model learns effectively as the number of iterations increases. The higher the accuracy, the higher the reliability of the model in performing the classification assignment and vice versa. Although a slight drop in the accuracy was observed at about 110 which might be due to the effect of overfitting, however, the model shows constant accuracy from the 120th iteration to 200. This indicates that the model is reliable and efficient in performing the classification task. Each iteration estimates the gradient and updates of the network parameters. Furthermore, the training loss plot indicates that the loss decrease steadily as the number of iteration increases which indicates that the models learns effectively over time.

FIGURE 8, displays the confusion matrix of the CNN model. The output ad target class “1”, “2” and “3” represent “banking applications”, “online banking”, and “mobile banking” respectively. The first row and first column of the overall confusion matrix represent the classification of fraud under “banking applications” while second row and second column represent “online banking” and the third row and third column for “mobile banking”. The CNN model correctly predicted 130 “True Positive” fraud cases classified as “Banking Applications” without any incorrect predictions. Looking at the “banking applications” column (first column). 22 fraud cases that actual belong to the “banking applications” class were wrongly classified as “online banking and 14 fraud cases that also belong to the “banking applications” were grouped as mobile banking”. These misclassification are referred as “False Positive”. For the banking applications”, the percentage of correct classification 78.3% with 21.7% incorrect classifications.

Looking at the second column (Online banking), 15 fraud cases that belong to “online banking” were incorrectly classified as “banking applications” while 325 fraud cases were incorrectly classified as “mobile banking” instead of “online banking”. Only 28 fraud cases were correctly classified as “online banking”. Therefore, the percentage of correct classification was 7.6% with 92.4% incorrect classifications for “online banking”.

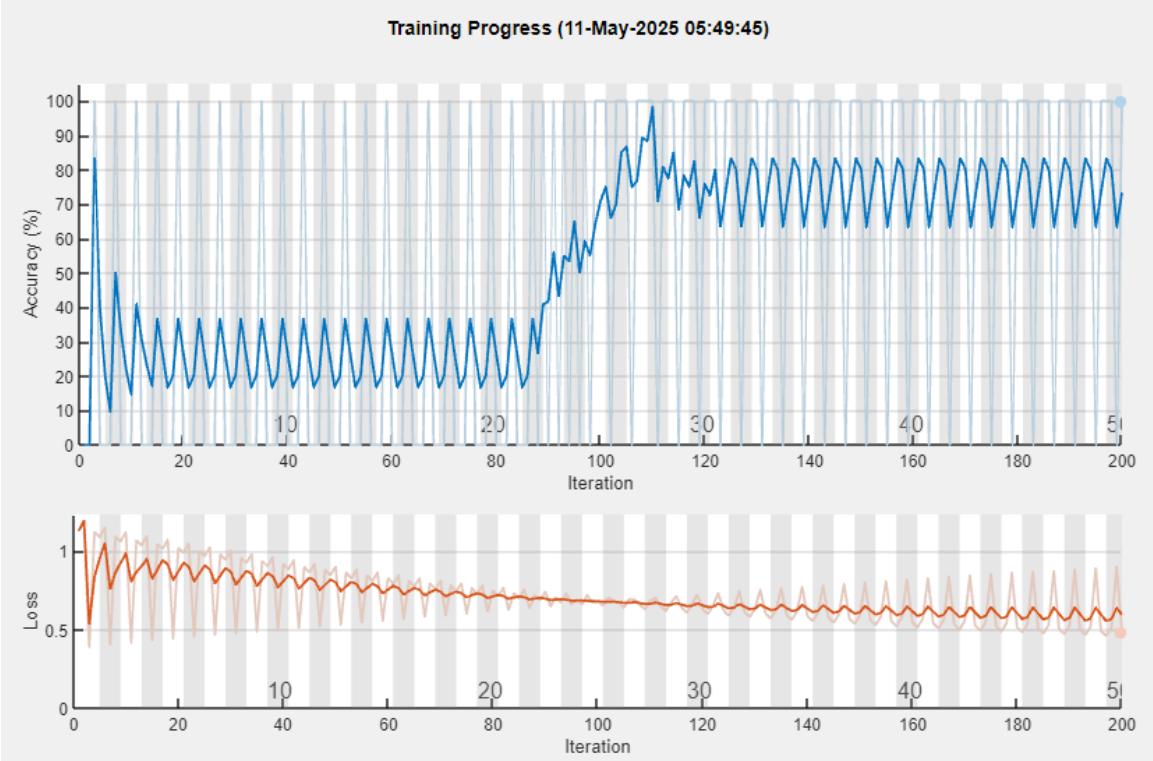

Figure 7: The progress of the training of the CNN model

For the third column (mobile banking), 13 fraud cases that belong to "mobile banking" incorrectly classified as "banking applications" while 20 cases were also wrongly classified as "online banking". However, 6633 fraud cases were correctly classified as "mobile banking". Thus, the percentage of correct classification was 99.5% with 0.5% incorrect classifications for "mobile banking". On the overall, there was 94.3% correct classification as opposed to 5.7% incorrect classifications using the CNN model.

From FIGURE 4, for the first class (banking applications): True Positive (TP) = 130, while True Negative (TN) equals to =7200-130-36-28=7006. False Positive (FP) equals to 22+14=36, while False Negative (FN) equals to 15+13= 28.

For the second class (Online banking): True Positive (TP) = 28, while True Negative (TN) equals to 7200-28-340-52=6780. False Positive (FP) equals to 15+325=340, while False Negative (FN) equals to 22+20= 52.

For the third class (Mobile banking): True Positive (TP) = 6633, while True Negative (TN) equals to 7200-6633-33-339=195. False Positive (FP) equals to 13+20=33, while False Negative (FN) equals to 14+325= 339.

Therefore, using equations 2-5, the accuracy, precision, recall and F1-score of the CNN classification model are computed and presented for each class in TABLE 4.

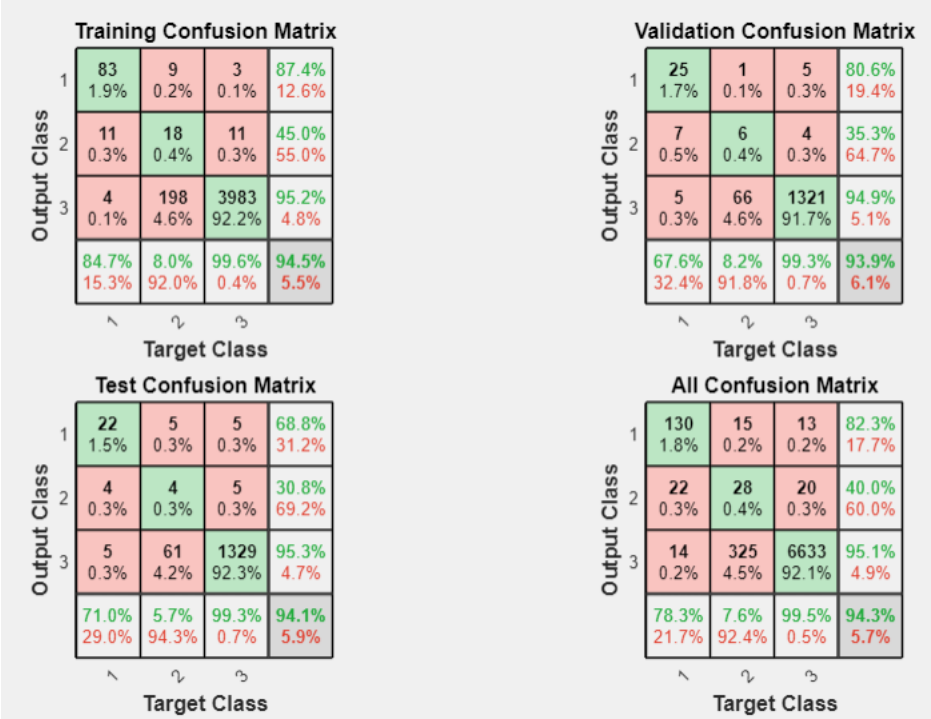

Figure 8: The confusion matrix of the CNN model.

Table 4: Evaluation metrics computation for the CNN model

Class	Evaluation metrics			
	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Class 1: Banking applications	99.11	78.31	82.28	80.20
Class 2: Online banking	94.56	7.61	35.00	13.0
Class 3: Mobile banking	94.83	99.50	95.14	97.26
Average	96.17	61.80	70.81	63.49

4.2 Multi Classification of Cyberfraud Incidences using the LSTM Model

FIGURE 9, shows the progress of the training of the LSTM model for 400 iterations. The iteration terminated at 100 epochs after the convergence of the solution without over fitting. The accuracy plot expressed in percentage indicates that the accuracy of the model increases from initial value of 30% to over 80% as the number of iterations increases which indicates that the model learns effectively as the number of iterations increases. The higher the accuracy, the higher the reliability of the model in performing the classification assignment and vice versa. The model also shows constant accuracy from the 20th iteration to 400. This indicates that the model is reliable and efficient in performing the classification task. Furthermore, the training loss plot indicates that the loss decreases slightly as the number of iteration increases which indicates that the models learns effectively over time.

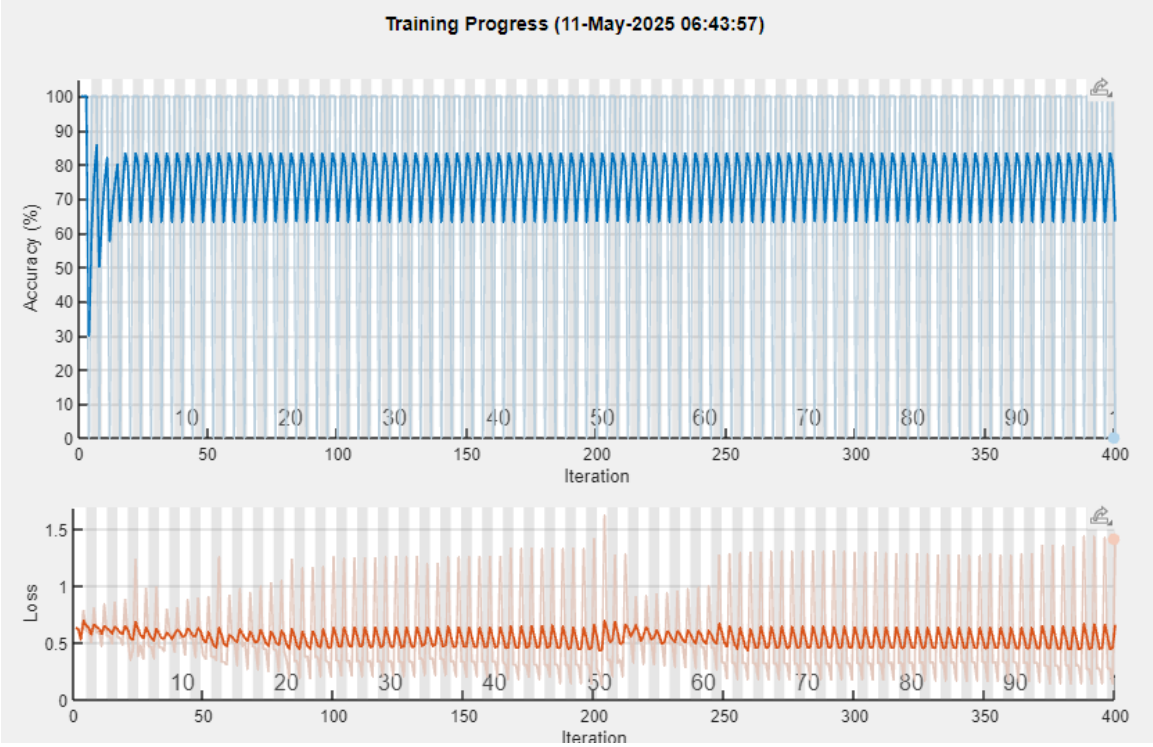

Figure 9: The progress of the training of the CNN model

FIGURE 10, presents the confusion matrix of the LSTM model. The output ad target class "1", "2" and "3" represent "banking applications", "online banking", and "mobile banking" respectively. Considering the overall confusion matrix, the first row and first column of the represent the classification of fraud under "banking applications" while second row and second column represent "online banking" and the third row and third column for "mobile banking". The LSTM model correctly predicted 130 "True Positive" fraud cases classified as "Banking Applications" without any incorrect predictions. Looking at the "banking applications" column (first column). 21 fraud cases that actual belong to the "banking applications" class were wrongly classified as "online banking and 15 fraud cases that also belong to the "banking applications" were grouped as mobile banking". These misclassification are referred as "False Positive". For the banking applications", the percentage of correct classification 78.3% with 21.7% incorrect classifications.

Looking at the second column (Online banking), 4 fraud cases that belong to "online banking" were incorrectly classified as "banking applications" while 222 fraud cases were incorrectly classified as "mobile banking" instead of "online banking". Only 142 fraud cases were correctly classified as "online banking". Therefore, the percentage of correct classification was 38.6% with 61.4% incorrect classifications for "online banking".

For the third column (mobile banking), 17 fraud cases that belong to "mobile banking" incorrectly classified as "banking applications" while 15 cases were also wrongly classified as "online banking". However, 6634 fraud cases were correctly classified as "mobile banking". Thus, the percentage of correct classification was 99.5% with 0.5% incorrect classifications for "mobile banking". On the

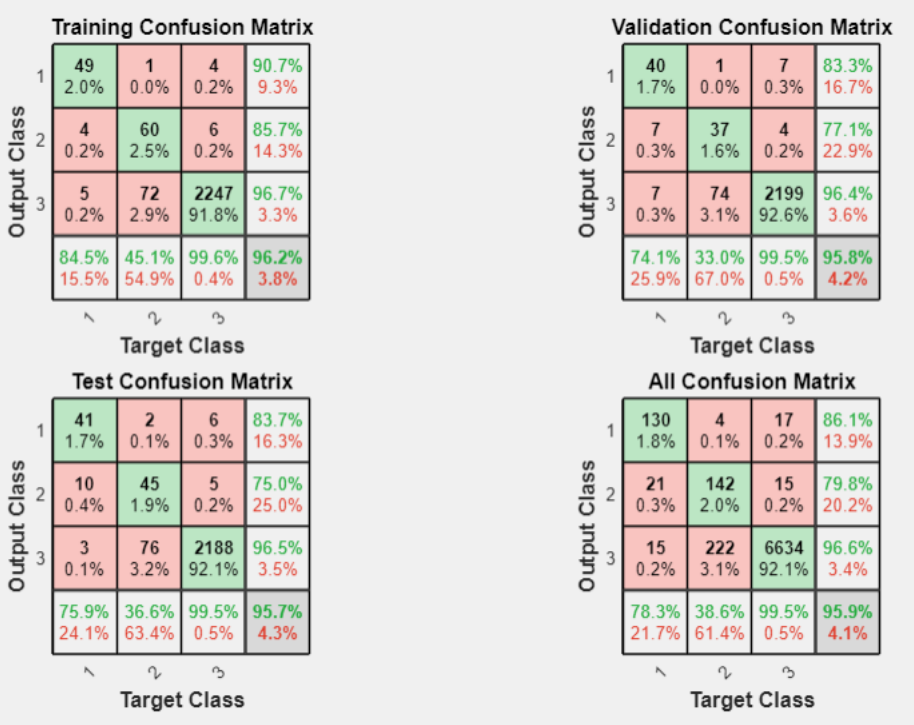

Figure 10: The confusion matrix of the LSTM model.

overall, there was 99.5% correct classification as opposed to 0.5% incorrect classifications for the LSTM model.

From FIGURE 10, for the first class (banking applications): True Positive (TP) = 130, while True Negative (TN) equals to =7200-130-36-21=7013. False Positive (FP) equals to 21+15=36, while False Negative (FN) equals to 4+17= 21

For the second class (Online banking): True Positive (TP) = 142, while True Negative (TN) equals to 7200-142-226-36=6796. False Positive (FP) equals to 4+222=226, while False Negative (FN) equals to 21+15= 36.

For the third class (Mobile banking): True Positive (TP) = 6634, while True Negative (TN) equals to 7200-6634-32-247=287. False Positive (FP) equals to 17+15=32, while False Negative (FN) equals to 15+222= 247.

Therefore, using equations 2-5, the accuracy, precision, recall and F1-score of the LSTM classification model are computed and presented for each class in TABLE 5.

The results obtained for cyberfraud classification using the LSTM model in this study fell within the range of the results obtained in the literature for intrusion detection using similar performance metrics reported by existing studies [64, 65, 67, 70, 71]. These studies considered DL models with high values of accuracy (greater than 70%) as a high performing model. However, the result obtained for the CNN model fell slightly below the benchmark of 70% in terms of precision and

Table 5: Evaluation metrics computation for the LSTM model

Class	Evaluation metrics			
	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Class 1: Banking applications	99.21	78.31	86.10	82.01
Class 2: Online banking	96.36	38.59	79.78	52.0
Class 3: Mobile banking	94.83	99.52	96.41	97.93
Average	96.80	72.14	87.43	77.31

F1-score. This implies that the LSTM outperform the CNN model in the classification task. This is clearly displayed in the comparative analysis shown in FIGURE 11. As a result, the LSTM model was further employed for the time series analysis.

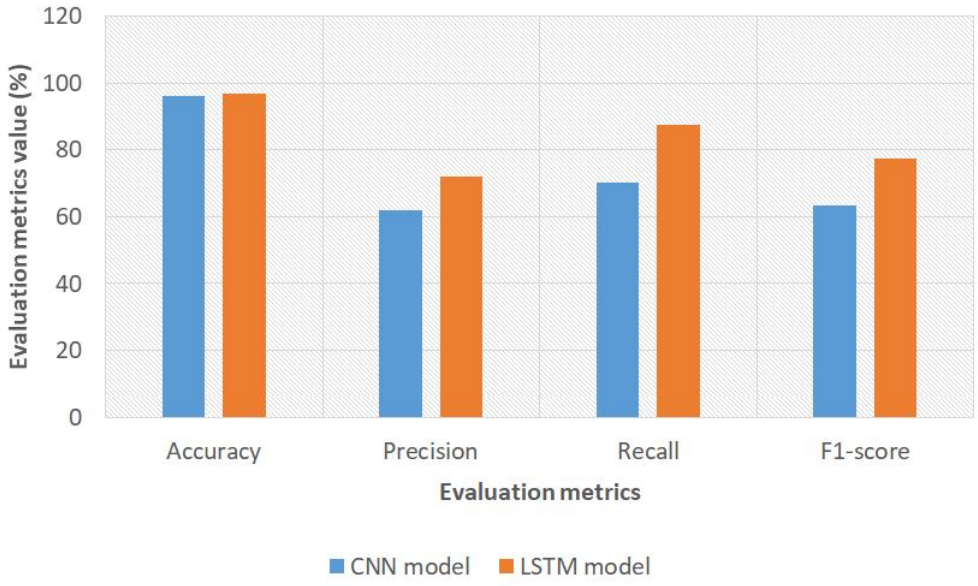

Figure 11: Comparative analysis of the performance of the CNN and LSTM model

4.3 Time Series Prediction using the LSTM Model

FIGURE 12, displays the time series analysis of the cyberfraud fraud cases from 2018-2023 using the LSTM model. The essence is to visualise the trend of the cyberfraud cases during the evaluated period and make predictions for the next six years. FIGURE 11, shows that the normalised value depicting the severity resulting from the occurrence of cyberfraud in terms of gross loss increases from 2018-2023 and the severity is projected to increase over the next six years (till 2030). Severity normalised values of 0.68, 0.71, 0.74, 0.76, 0.78 and 0.80 were predicted for 2025 to 2030 respectively. This analysis agrees significantly with the SABRIC annual reports [10, 15–19], which indicates an increase in the trend and rate of cyberfraud perpetration and the resulting loses. This increase in the rate of perpetration of cyberfraud and resulting loses in South Africa may be due to

the sophistication and dynamics of the threat actors in social engineering activities such as malware, phishing, smishing, vishing, SIM swap etc. to obtain sensitive information from individuals or organisations for fraud perpetration across the banking digital channels. Threat actors also exploit vulnerabilities in the internal controls of the banking institutions such as inadequate to commit fraud [16–19].

The results obtained in in line with the outcome of existing studies such as Mbelli and Dwolatzky [79], identify lack of effective supervision and control as some of the reasons for cyberfraud perpetration and that cyber insecurity remains a threat to the South African banking industry. Existing authors also acknowledge the increasing rate of cybercrime perpetration and impact especially in the banking and financial sector due to weak response, controls and legal framework which increases the cost of cybercrime and promotes customer dissatisfaction [80–83].

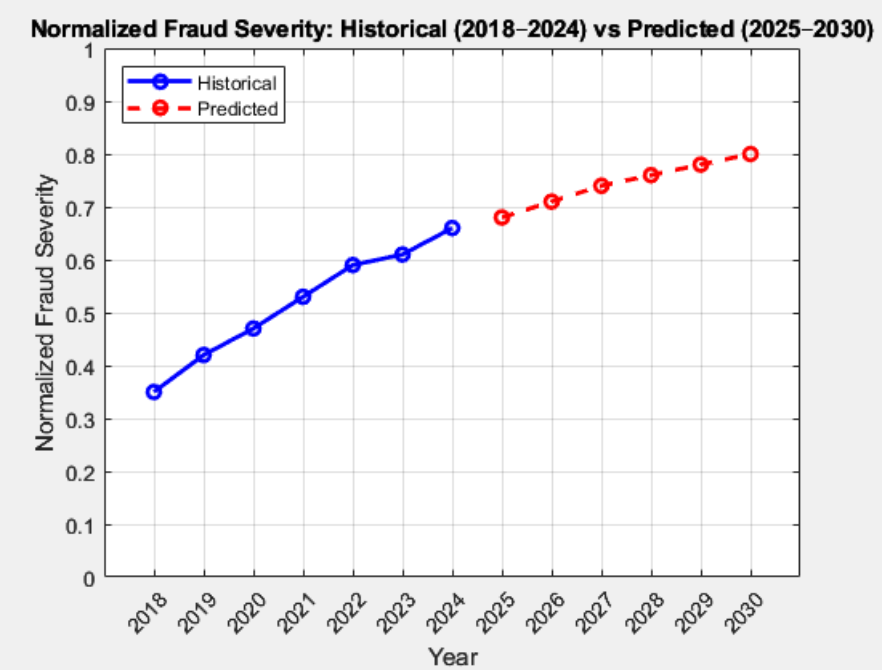

Figure 12: The time series prediction of cyberfraud cases using LSTM model.

4.4 Integration of Deep Learning (DL) into the Cybersecurity Architecture of Financial Institutions

This study demonstrates the application of the DL model, specifically the CNN and LSTM model for cyberfruad classification. The model have the ability to identify complex and hidden patterns and relationship that could lead to cyberfraud detection. It can also be used for forecasting future trends or severity of cyberfraud including financial savings or losses depending on the rate of cyberfraud perpetration. Compared to the conventional rule based approach of cyberfraud detection, the proposed DL approach and handle larger and complex dataset offering real tie detection of cyberfraud with high accuracy. The model can also adapt and update in real time which makes it effective in determining potential threats and fraud cases in real time. FIGURE 13, presents a conceptual

framework proposed in this study that can assist banking or financial institutions incorporate the DL technique into their existing cybersecurity architecture to enable real time classification and prediction of cyberthreats or fraud and their severity.

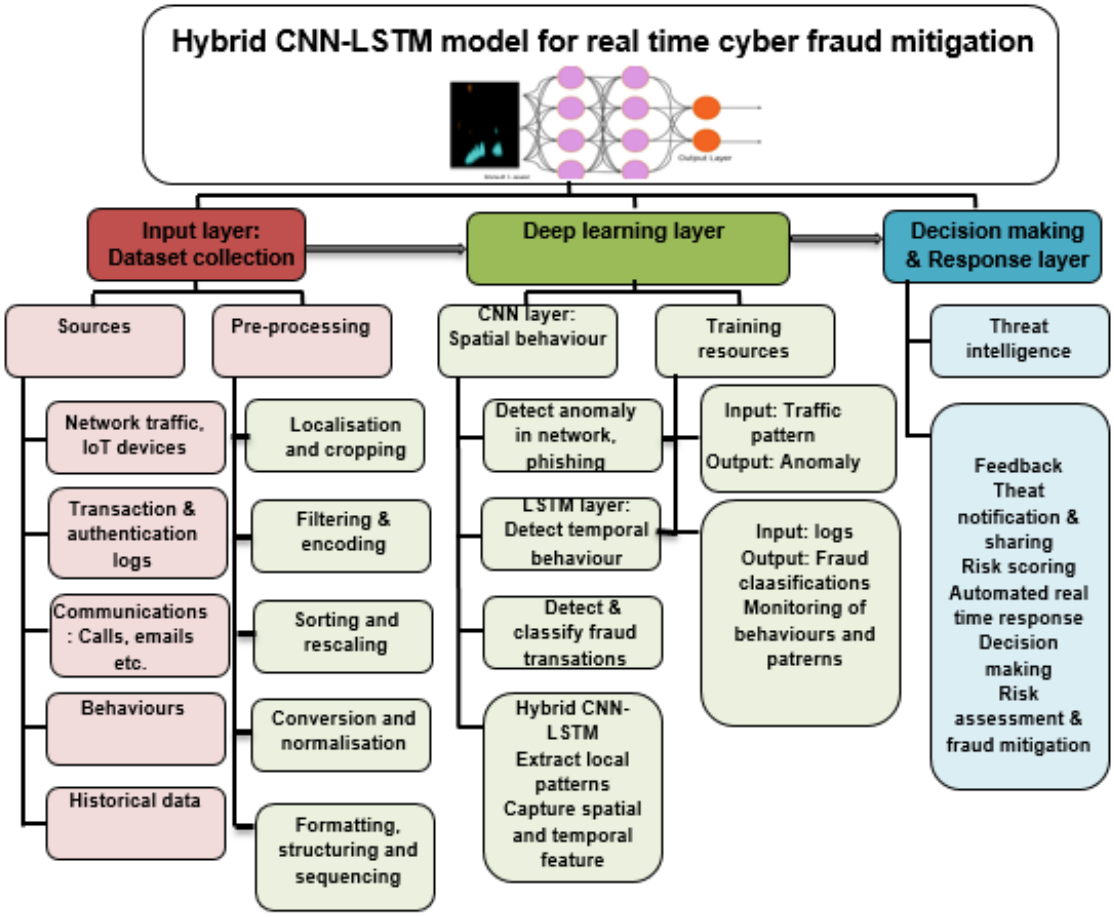

Figure 13: Hybrid CNN-LSTM model for real time cyber fraud mitigation

The framework shown in FIGURE 12, comprises of three major layers namely: the input layer, DL layer and decision making and response layer. The input layer details on data collection from different sources such as network , transaction, communication either real time or historical and preprocessing such as formatting, sequencing, sorting or conversion so that it will be compatible with DL structure. The proposed hybrid CNN-LSTM DL learning model has input and output layer depending on the nature of cyberfraud mitigation to be achieved. For instance, with the use of network traffic pattern, anomalies can be detected and with transaction or communication logs, fraud can be detected, classified and monitored. The integrated CNN-LSTM model can capture spatial and temporal behaviours and extract patterns necessary for fraud detection in real time. The last layer which is the decision making layer provides the output of the integrated model necessary for decision making and generating automation response such as blockage of a suspicious transactions in real time. It can also be deployed for threat intelligence and sharing, risk scoring and assessment amongst others.

5. POLICY IMPLICATIONS

The integration of DL based models such as CNN, LSTM etc. into the cybersecurtiy of financial institution offer significant benefits especially in the areas of real time fraud classification, detection and cyber risk management. However, there also some policy implications that must be considered ranging from regulatory compliance to disclosure as well as data privacy and other ethical considerations that revolve around the use of AI based models. Firstly, financial institutions must ensure that the use of the DL models complies with the regulatory standards under the auspices of the Financial Sector Conduct Authority (FSCA) and the South African Reserve Bank (SARB). For instance, the DL models must be auditable or compliant with the current audit processes of the institution and regulatory bodies. In terms of the legal requirements, the Protection of Personal Information Act (POPIA) 4 of 2013 of South Africa emphasised protection of data, highlights the conditions for lawful possession or processing of personal information and penalises data breaches while section 19-22 emphasises notification of data breaches [84]. The models must also be compliant with the Electronic Communication and Transaction Act 2002 of South Africa which governs electronic communications, e-commerce, data protection in cyberspace as well as offenses relating to cybercrime [85]. Thus the dataset employed for the development of DL models must be anonymised, lawfully acquired and used with informed consent in compliance with the POPIA. In terms of ethical requirements, AI models may be subject to bias depending on the nature of dataset employed for training. Hence, for instance, it can flag some normal transactions as suspicious due to incorrect classification and hence deny a lawful client holder access to account or transaction. Thus, proper documents of the AI-based decision and regular audits or review of the models are recommended. Furthermore, human oversights and internal control mechanisms may minimise the bias or misuse of such models. As threat and threat actors evolve over time, there may need for continuous monitoring and improvement of the AI-based models. This may also involve human capacity development in the area of AI. For instance, there is a critical skill gap in AI in South Africa thus effective coloration among academic and research institutions, as well as training of staff, may contribute to innovation and technology transfer needed to drive this proposed initiative. Furthermore, AI-based model must be aligned towards the local cybersecurity framework such as the framework of the South Africa's National Cybersecurity Policy Framework (NCPF) which requires data protection and proactive threat detection. In addition, AI based models thrive well in an environment with data driven culture and infrastructure. For instance the accuracy of the DL models depends on the data diversity, volume and integrity Thus, a system of data tracking, safe storage and sharing protocol must be established in compliance with the POPIA. Lastly, the deployment of AI-based models to enhance cybersecurity requires the synergy of the stakeholders such as government, financial institutions, network providers, regulatory bodies, law enforcement agencies etc.

6. CONCLUSION AND RECOMMENDATIONS

This study applies the DL technique for cyberfraud mitigation using secondary data obtained from SABRIC from 2018-2023. The data was trained under the DL paradigm using the CNN and LSTM models and adaptive moment estimation (ADAM) algorithm for fraud incidence classification and time series prediction of fraud incidences.

On the overall, the LSTM model with an accuracy of 96.80% outperformed the CNN model with an overall accuracy of 96.17%. Moreover, the accuracy, precision, recall and F1-score of the LSTM classification model namely 72.14%, 87.43% and 77.31% respectively exceeded 70%. The results show that the LSTM model can be deployed for fraud classification and time series analysis of fraud incidences. The outcome of this study may promote cyber resilience and sustain the fight against the perpetration of cyber-related fraud in the South Africa. The use of the DL model for cyberfraud classification and time series prediction of cyberfraud incidences demonstrated in this study is unique. This study contributes conceptually, theoretically and empirical to knowledge on cyberfraud mitigation. It proposes an AI based conceptual framework for reinforcing cybersecurity in the financial institution. It also develops a conceptual framework and offers useful insight that can assist the South African financial institutions in combating cyberfraud. Therefore, the integration of the DL techniques such as the CNN and LSTM into the cyber-risk assessment framework of financial institutions are recommended. However, the potentials of these DL approaches can be fully harnessed with the availability of robust dataset, consistent model updates, integration with other compatible data analytic techniques amongst others. This study is limited to the use of the CNN and LSTM algorithm for fraud incidences classification, future works can consider a comparative analysis of different hybrid DL and recurrent neural models. The fraud detection and predictive capability of the proposed hybrid CNN-LSTM framework can be further explored to promote the cyberfraud mitigation in banking and financial institutions.

7. DECLARATION

- Availability of data and materials: The data that support will be made available by the corresponding author upon a reasonable request.
- Competing Interests: The authors declare no conflict of interest.
- Funding: No funding was received.

References

[1] Maduku DK. The Effect of Institutional Trust on Internet Banking Acceptance: Perspectives of South African Banking Retail Customers. S Afr J Econ Manag Sci. 2016;19:533-548.

[2] Jara AJ, Parra MC, Skarmeta AF. Participative Marketing: Extending Social Media Marketing Through the Identification and Interaction Capabilities From the Internet of Things. Pers Ubiquitous Comput. 2014;18:997-1011.

[3] Tran HT, Corner J. The Impact of Communication Channels on Mobile Banking Adoption. Int J Bank Mark. 2016;34:78-109.

[4] Nel J, Boshoff C. Enhancing the Use of Internet Banking in an Emerging Market. S Afr J Econ Manag Sci. 2014;17:624-638.

[5] Singh S, Srivastava RK. Predicting the Intention to Use Mobile Banking in India. Int J Bank Mark. 2018;36:357-378.

[6] Akinbowale OE, Klingelhöfer HE, Zerihun MF. The Assessment of the Impact of Cyberfraud in the South African Banking Industry. J Financ Crime. 2024;31:287-301.

[7] Akinbowale OE, Klingelhöfer HE, Zerihun MF. Analytical Hierarchy Process Decision Model and Pareto Analysis for Mitigating Cybercrime in the Financial Sector. J Financ Crime. 2022;29:884/984-1008.

[8] Koto C, Smith RJ, Schutte B. Cyber Risk Management Frameworks for the South African Banking Industry. 6th Annual International Conference on Public Administration and Development Alternatives. University of Venda. 2021:80-89.

[9] Akinbowale OE, Klingelhöfer HE, Zerihun MF. Analysis of Cyber-Crime Effects on the Banking Sector Using Balance Score Card: A Survey of Literature. J Financ Crime. 2020;27:945-958.

[10] https://www.sabric.co.za/media/vjyn5f4d/sabric-annual-crime-stats-2023-2.pdf

[11] https://www.resbank.co.za/content/dam/sarb/publications/reviews/finstab-review/2020/financial-stability-review-2nd-edition-2020/Second%20edition%202020%20Financial%20Stability%20Review.pdf

[12] https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa

[13] https://kaspersky.africa-newsroom.com/press/africa-remains-one-of-the-regions-most-targe
lang=en#:~:text=In%20QQ3%202023%2C%20according%20to,ICS%20machines%20in%20Q3%202023

[14] https://surfshark.com/research/data-breach-impact/statistics

[15] https://www.sabric.co.za/media/vq0dyizx/sabric-annual-crime-stats-2018.pdf

[16] https://www.sabric.co.za/media/qz1eiq4p/sabric-annual-crime-stats-2019.pdf

[17] https://www.sabric.co.za/media/20oouwbg/sabric-annual-crime-stats-2020.pdf

[18] https://www.sabric.co.za/media/z0vch20l/sabric-annual-report-2021.pdf

[19] https://www.sabric.co.za/media/gq4hmbjw/sabric-annual-crime-stats-2022.pdf

[20] https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime

[21] https://www.news24.com/tech-and-trends/csir-collaborates-with-saps-to-strengthen-cybercr

[22] https://www.fic.gov.za/wp-content/uploads/2023/09/2022.8-MR-Fusion-Centre-marks-two-years-of-successful-private-public-collaboration.pdf

[23] https://www.pwc.com/ua/en/survey/2020/economic-crime-survey.html

[24] https://www.pwc.dk/da/presse/2018/gecs-2018.pdf

[25] Almuhammadi S, Alsaleh M. Information Security Maturity Model for Nist Cyber Security Framework. Comput Sci Inf Technol. 2017;7:51-62.

[26] Abbas S, Alsubai S, Ojo S, Sampedro GA, Almadhor A, et al. An Efficient Deep Recurrent Neural Network for Detection of Cyberattacks in Realistic Iot Environment. J Supercomput. 2024;80:13557-13575.

[27] Raza SA, Umer A, Qureshi MA, Dahri AS. Internet Banking Service Quality, E-Customer Satisfaction and Loyalty: The Modified E-SERVQUAL Model. TQM J. 2020;32:1443-1466.

[28] Nkoyi A, Tait M, Van der Walt F. Predicting the Attitude Towards Electronic Banking Continued Usage Intentions Among Rural Banking Customers in South Africa. S Afr J Inf Manag. 2019;21:1-8.

[29] Akinbowale OE, Klingelhöfer HE, Zerihun MF, Mashigo P. Emerging Technologies as a Mediating Factor Between Causes of Cyberfraud and Cyberfraud Perpetration in the South African Banking Industry. Int J Cyber Behav Psychol Learn. 2025;15:1-19.

[30] Ali L, Ali F, Surendran P, Thomas B. The Effects of Cyber Threats on Customer's Behaviour in E-banking Services. Int J e-Educ e-Bus e-Manag e-Learn. 2017;7:70-78.

[31] Maduku DK. Predicting Retail Banking Customers Attitude Towards Internet Banking Services in South Africa. South Afr Bus Rev. 2013;17:76-100.

[32] Raza SA, Hanif N. Factors Affecting Internet Banking Adoption Among Internal and External Customers: A Case of Pakistan. Int J Electron Fin. 2013;7:82-96.

[33] Yu J, Guo C. An exploratory study of applying ubiquitous technology to retail banking. In Allied Academies International Conference. Academy of Banking Studies. Proceedings 2008. Jordan Whitney Enterprises, Inc. 2008;8:7-12.

[34] Ngai EW, Hu Y, Wong YH, Chen Y, Sun X. The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature. Decis Support Syst. 2011;50:559-569.

[35] West J, Bhattacharya M. Intelligent Financial Fraud Detection: A Comprehensive Review. Comput Sec. 2016;57:47-66.

[36] Ismail Fawaz HI, Forestier G, Weber J, Idoumghar L, Muller PA. Deep Learning for Time Series Classification: A Review. Data Min Knowl Discov. 2019;33:917-963.

[37] Roy A, Sun J, Mahoney R, Alonzi L, Adams S, et al. Deep Learning Detecting Fraud in Credit Card Transactions. Systems and Information Engineering Design Symposium. Charlottesville, VA, USA. 2018:129-134.

[38] Iscan C, Akbulut FP. Fraud Detection Using Recurrent Neural Network for Digital Wallet Security. 8th IEEE International Conference on Computer Science & Engineering Burdur Turkey. 2023:538-542.

[39] Hernandez Aros L, Bustamante Molano LX, Gutierrez-Portela F, Moreno Hernandez JJ, Rodríguez Barrero MS. Financial Fraud Detection Through the Application of Machine Learning Techniques: A Literature Review. Humanit Soc Sci Commun. 2024;11:1-22.

[40] Redlinghuis A, Rensleigh C. Customer Perceptions on Internet Banking Information Protection. S Afr J Inf Manag. 2010;12:1-6.

[41] https://iol.co.za/sundayindependent/news/2021-05-30-the-scary-nature-of-cybercrimes-and-the-strain-of–bringing-perpetrators-to-book/

[42] Hubbard J. SA Business Underplaying the Danger of Cybercrime? Finweek. 2019;4:37-38.

[43] Kundu S, Islam KA, Jui TT, TT, Rafi S, Hossain MA et al. Cyber Crime Trend in Bangladesh an Analysis and Ways Out to Combat the Threat. 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon South Korea. IEEE. 2018;474-480.

[44] Cassim F. Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players. Comparative and International Law Journal of Southern Africa. 2011;44:126-138.

[45] https://www.yumpu.com/en/document/view/38025407/banking-sector-overview-epic-communications

[46] https://iol.co.za/pretoria-news/news/2023-04-06-bleak-picture-painted-as-cybercrime-costs-sa-r2-2-billion-annually/

[47] Van Niekerk B. An analysis of cyber-incidents in South Africa. Afr J Inf Commun. 2017;20:113-132.

[48] Akinbowale OE, Klingelhöfer HE, Zerihun MF. The Integration of Forensic Accounting and the Management Control System as Tools for Combating Cyberfraud. Acad Acc Financ Stud J. 2021;25:1-14.

[49] https://www.resbank.co.za/content/dam/sarb/publications/shares-correspondence/2017/7860/Annual-Report-2016-17.pdf

[50] Akinbowale OE, Zerihun MF, Mashigo P. Banking and Financial Regulation in Sub-Saharan Africa: A Systematic Literature Review and Multiple Regression Approach. J Financ Regul Compliance. 2025;33:359-385.

[51] Thamae RI, Odhiambo NM, Khumalo JM. Bank Regulation in the Selected Subsaharan African Countries: Dynamics and Trends. J Cent Banking Theor Pract. 2023;12:175-198.

[52] https://documents1.worldbank.org/curated/en/685851571160819618/pdf/Bank-Regulation-and-Supervision-Ten-Years-after-the-Global-Financial-Crisis.pdf

[53] http://www.bsg.ox.ac.uk/research/developing-countries-navigating-global-banking-standards

[54] Cerutti E, Claessens S, Laeven L. The Use and Effectiveness of Macroprudential Policies: New Evidence. J Financ Stab. 2017;28:203-224.

[55] Jones E, Zeitz AO. The Limits of Globalizing Basel Banking Standards. J Financ Regul. 2017;3:89-124.

[56] Evdokimova Y, Shinkareva O, Egorova E. Banking Information Technology as an Element of the Information Society. 54th International Scientific Conference on Economic and Social Development. International Social Congress. Moscow. 2019;19:550-555.

[57] Snail Ka Mtuze S, Musoni M. An Overview of Cybercrime Law in South Africa. Int Cybersecur Law Rev. 2023;4:1-25.

[58] https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104

[59] Dzomira S. Internet Banking Fraud Alertness in the Banking Sector: South Africa. Banks Bank Syst. 2017;12:143-151.

[60] Dlamini Z, Modise M. Cyber Security Awareness Initiatives in South Africa: A Synergy Approach. 7th International Conference on Information Warfare and Security Seattle USA. 2012;1:98-107.

[61] Davis FD. Perceived Usefulness Perceived Ease of Use and User Acceptance of Information Technology. MIS Q. 1989;13:319-340.

[62] Chandola V, Banerjee A, Kumar V. Anomaly detection: A survey. ACM Comput Surv. 2009;41:1-58.

[63] Chandran PP, Rajini NH, Jeyakarthic M. Optimal Deep Belief Network Enabled Malware Detection and Classification Model. Intell Autom Soft Comput. 2023;35:3349-3364.

[64] Shende S, Thorat S. Long Short-Term Memory (LSTM) Deep Learning Method for Intrusion Detection in Network Security. Int J Eng Res Technol. 2020;9:1615-1620.

[65] Jony AI, Arnob AK. A Long Short-Term Memory Based Approach for Detecting Cyber Attacks in Iot Using Cic-IOT2023 Dataset. J Edge Comp. 2024;3:28-42.

[66] Saxe J, Berlin K. Deep Neural Network Based Malware Detection Using Two Dimensional Binary Program Features. 10th International Conference on Malicious and Unwanted Software (MALWARE), Fajardo PR USA. 2015:11-20.

[67] Awad AA, Ali AF, Gaber T. An Improved Long Short Term Memory Network for Intrusion Detection. PLOS One. 2023;18:e0284795.

[68] Ibitoye O, Shafiq O, Matrawy A. Analyzing Adversarial Attacks Against Deep Learning for Intrusion Detection in Iot Networks. IEEE Global Communications Conference (GLOBECOM). IEEE. 2019:1-6.

[69] Dhanya KA, Vajipayajula S, Srinivasan K, Tibrewal A, Kumar TS, et al. Detection of Network Attacks Using Machine Learning and Deep Learning Models. Procedia Comput Sci. 2023;218:57-66.

[70] Kolosnjaji B, Zarras A, Webster G, Eckert C. Deep Learning for Classification of Malware System Call Sequences. Lect Notes Comput Sci AI: Advances in Artificial Intelligence. 2016;9992:137-149.

[71] Rhode M, Burnap P, Jones K. Early-Stage Malware Prediction Using Recurrent Neural Networks. Comput Sec. 2018;77:578-594.

[72] HaddadPajouh H, Dehghantanha A, Khayami R, Choo KK. A Deep Recurrent Neural Network Based Approach for Internet of Things Malware Threat Hunting. Future Gener Comput Syst. 2018;85:88-96.

[73] Halbouni A, Gunawan TS, Habaebi MH, Halbouni M, Kartiwi M, et al. CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System. IEEE Access. 2022;10:99837-99849.

[74] Hnamte V, Hussain J. DCNNBiLSTM: An Efficient Hybrid Deep Learning-Based Intrusion Detection System. Telemat Inform Rep. 2023;10:100053.

[75] Qazi EU, Faheem MH, Zia T. HDLNIDS: Hybrid Deep-Learning-Based Network Intrusion Detection System. Appl Sci. 2023;13:4921.

[76] Lan J, Liu X, Li B, Sun J, Li B, et al. Member: A Multi-Task Learning Model With Hybrid Deep Features for Network Intrusion Detection. Comput Sec. 2022;123:102919.

[77] Sutherland E. Governance of Cybersecurity-the Case of South Africa. Afr J Inf Commun. 2017;20:83-112.

[78] Al-Garadi MA, Mohamed A, Al-Ali AK, Du X, Ali I, et al. A Survey of Machine and Deep Learning Methods for Internet of Things (Iot) Security. IEEE Commun Surv Tutorials. 2020;22:1646-1685.

[79] Mbelli TM, Dwolatzky B. Cyber Security a Threat to Cyber Banking in South Africa: An Approach to Network and Application Security. IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud) Beijing China. 2016:1-6.

[80] Kraemer-Mbula E, Tang P, Rush H. The Cybercrime Ecosystem: Online Innovation in the Shadows? Technol Forecasting Soc Change. 2013;80:541-555.

[81] Lagazio M, Sherif N, Cushman M. A Multi-Level Approach to Understanding the Impact of Cybercrime on the Financial Sector. Comput Sec. 2014;45:58-74.

[82] Raza SA, Jawaid ST, Hassan A. Internet Banking and Customer Satisfaction in Pakistan. Qual Res Financ Markets. 2015;7:24-36.

[83] Saini H, Rao YS, Panda TC. Cyber-Crimes and Their Impacts: A Review. Int J Eng Res Appl. 2012;2:202-209.

[84] https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

[85] Available at : https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf