South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

Online banking fraud detection: A comparative study of cases from South Africa and Spain

Authors:
Joy Phiri[1]
Tendani Lavhengwa[1]
Mmatshuene A. Segooa[1]

Affiliations:
[1]Department of Informatics, Faculty of Information and Communication Technology, Tshwane University of Technology, Tshwane, South Africa

Corresponding author:
Joy Phiri,
mjoyana@gmail.com

Dates:
Received: 06 Sept. 2023
Accepted: 08 Dec. 2023
Published: 20 Mar. 2024

How to cite this article:
Phiri, J., Lavhengwa, T. & Segooa, M.A., 2024, 'Online banking fraud detection: A comparative study of cases from South Africa and Spain', *South African Journal of Information Management* 26(1), a1763. https://doi.org/10.4102/sajim.v26i1.1763

Background: The banking sector provides online banking to offer their customers convenient and easy access to banking services. As most banking services are nowadays performed online, alarming fraudulent activities occur daily. The online banking frauds are increasingly and commonly being experienced globally and are damaging to both banks and customers.

Objectives: The goal of the study was to investigate issues in online fraud detection in the banking sector from South Africa and Spain.

Method: The study followed the Design Science Research (DSR) methodology. Data were collected through the qualitative approach particularly using focus groups and semi-structured interviews. The study followed non-probability sampling since it focussed on a specialised area of online fraud model. In total, the population size consisted of 17 participants, which included fraud technical managers, fraud investigator specialists, fraud technical specialists and data scientists.

Results: In the South African context, the study established that there is a lack of online fraud experts in the banking sector. The findings reveal that the lack of online fraud expertise may lead to banks having weak detection systems. In the Spanish perspective, the study revealed that there is a lack of law regulation that poses a high risk.

Conclusion: Given the lack of online fraud experts in the banking sector, banks are urged to acquire and develop online fraud expertise. Online banking technology is developing expeditiously than traditional transactions; therefore, regulations and policies need to be updated regularly to keep up with rapidly evolving technological changes.

Contribution: Considering the significance of global online banking, the study suggested areas that the banking sector may investigate to develop and enhance online fraud detection models to combat online fraudulent activities.

Keywords: banking sector; online banking; online banking fraud; fraud detection; fraud experts.

Introduction

The banking sector plays a significant role in the present-day generation, since practically every person deals with bank (John et al. 2016). A study conducted by Damrongsakmethee and Neagoe (2017) reveals that there has since been a transformation in which the banking sector operates, with the majority of functions being operated online. The typical in-person customer service has been replaced by online banking applications to speed up and lower the costs of processing various banking services and products. Online banking transactions along with technological developments produce huge amounts of data that often exceed bank employees' expertise. Because of the rise of online banking transactions, there has been a massive increase in online frauds also in the banking sector (Balasupramanian, Ephrem & Al-Barwani, 2017). Despite the banking sector's best efforts to create a reliable online banking environment for customers to conduct secure online banking transactions, online banking frauds persist.

Online banking fraud refers to the unauthorised use of a person's private information to make purchases or withdraw money from their account (Carneiro, Figueira & Costa 2017). Online banking fraud has become a major problem in the management of financial crime for the entire banking sector. The literature reveals that online frauds are growing at an unprecedented rate, leading to annual losses of billions of rands for both customers and the banking sector (Daliri 2020). Because of the ever evolving sophisticated online banking frauds, it is becoming increasingly difficult for the banking sector to manage them thus continuously causing

significant losses. Although the banking sector has made considerable efforts to secure its online banking applications, evidently huge annual losses are still rising because of online banking fraud (Singla & Jangir 2020). To deal with this eminent problem, Thennakoon et al. (2019) discovered that online banking fraud can be avoided in two ways: fraud prevention and fraud detection models. Fraud prevention evades any attacks from fraudsters by functioning as a layer of protection, whereas fraud detection occurs after prevention has failed.

Therefore, fraud detection models assist in identifying and alerting when a fraudulent transaction is triggered (Thennakoon et al. 2019). These models mostly focus on monitoring the customer's behaviour to detect anomalous access. In addition, Minastireanu and Mesnita) 2019) suggested fraud detection model as a way of combating online banking fraud. They demarcated fraud detection as security measures to avoid unauthorised individuals from originating transactions on an account to which they are not authorised to. The literature reveals that various online fraud detection models have been developed; however, these models have not been evaluated to identify recurring online fraud detection issues to assist the baking sector combat online fraud. Therefore, this study investigate issues for online fraud detection in the banking sector looking at cases from South Africa and Spain.

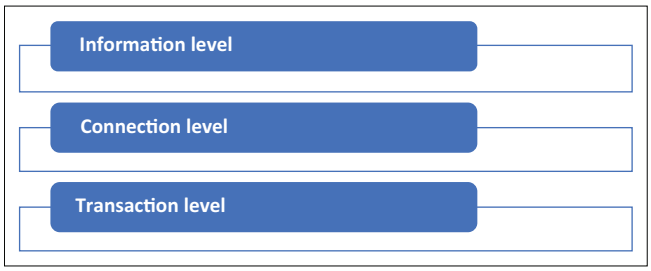
The article presents a comprehensive review of problems and challenges for online fraud detection in the banking sector. These problems and challenges were facilitated using the design science research (DSR) methodology (Gregor & Hevner 2013). The study intends to contribute to expanding information system research in the banking sector. It has adapted the current DSR processes to deliver higher quality study results appropriate to the context of the research. The theoretical contribution of the study addresses the improvement of solution maturity, which aims to develop new solutions for known problems (Gregor & Hevner 2013).

Literature

Online banking overview

The online banking refers to a platform that offers all traditional banking transactions conducted over the Internet through the customer's banking website. The Internet provides greater flexibility for people to communicate than the physical world that has lots of unchangeable limits (Krishnan 2017). The banking sector makes use of the Internet to provide online banking to customers. Through online banking, banks have been able to provide convenient and faster banking services to their customers. However, online banking services have not been smooth nor cheap to maintain because of online fraudulent activities (Raza et al., 2020). As shown in Figure 1, a typical online banking system has the following subsystems with varying access levels.

The information level provides non-sensitive information such as interest rates, branch locations, membership application forms, frequently asked questions (FQA) and any other business. No identification of users is required at information system level. The information level is the most uncomplicated stage in online banking (Rahi & Abd. Ghani 2019). The connection level gives read only, customer specific information including account balances, transaction records and account statements. Customers need to be identified and authenticated to access this part of the online banking system. It is slightly more advanced than the information level, providing full duplex connection between the bank and the customer (Raza et al. 2020). The transaction level requires customer identification details such as account number, login ID and password to access the right account and for authenticating a customer. This level enables the customer to update accounts such as when funds are transferred to a different account or when a payment is made. This is the most sophisticated online banking level in which transactions are also possible. All the traditional banking services are available through this level, which also comes with greater risks that requires advanced security systems (Rahi & Abd. Ghani 2019).



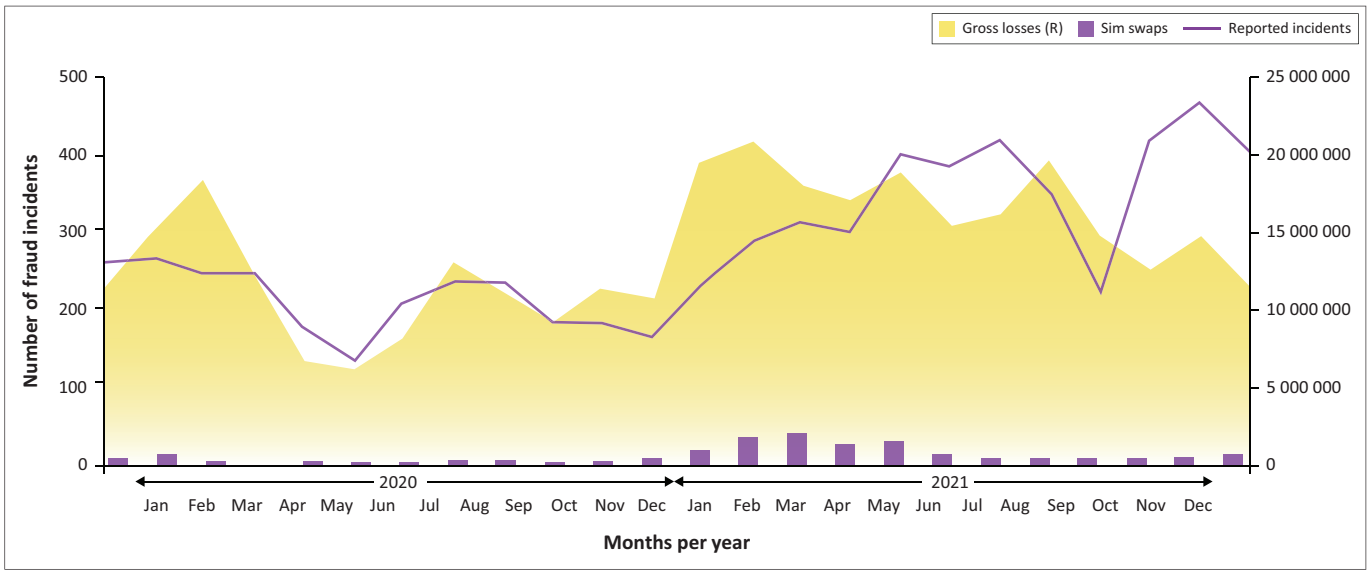
Source: Rahi, S. & Abd. Ghani, M., 2019, 'Investigating the role of UTAUT and e-service quality in internet banking adoption setting', *The TQM Journal* 31(3), 491–506

FIGURE 1: Levels of online banking system.

Online banking challenges

Undoubtedly, both banks and customers benefit in using online banking services. However, there are also challenges in ensuring security and privacy to fight against fraudulent activities. The banking sector and financial institutions endure yearly losses through online banking fraudulent crimes (Kumar, Mubarak & Dhanush 2020). The annual crime statistics shows that although the online banking fraud makes up the smallest portion of incidents of digital banking crime (20% of reported incidents), it accounts for the second highest portion of gross losses at 45% (SABRIC 2021).

Figure 2 provides yearly statistics on reports, which shows that online banking fraud crime allegations are rising every year with the reported incidents reaching 20 000 000 in 2021. It is important to note that when compared to bank application and mobile banking fraud, online banking fraud reflected the highest average financial value per incident. The online banking services risks and challenges must be mitigated to foster and preserve customer's trust. Online banking fraud has negative repercussions for all parties affected, this includes financial cost, inconvenience and loss of trust. From the literature review, studies identified few challenges related to online banking security that could result in fraud as discussed below:



Source: SABRIC, 2021, *Annual crime statistics 2021*, p. 1, viewed n.d., from www.sabric.com

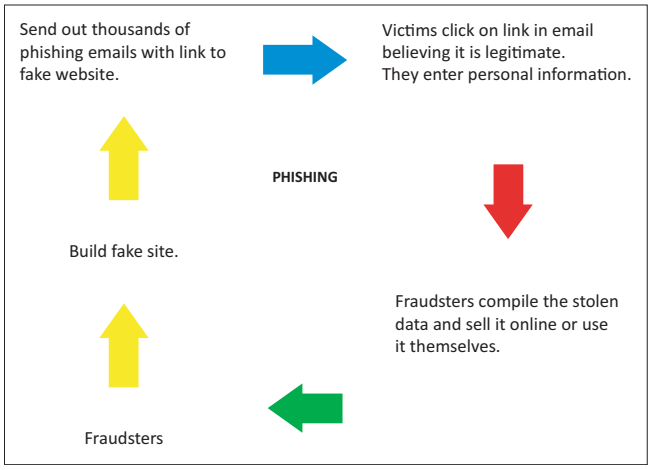
FIGURE 2: Online banking yearly statistics report.

- Lack of strong authentication – researchers have highlighted the necessity of having additional security measures to authenticate customer's identity on online banking application. When the same passwords are frequently used for many services, fraud vulnerability increases whenever such information is stolen (Shankar & Rishi 2020)
- Humans compromising security – customers and bank employees can both be considered as the weakest links in fraud. Several peoples use their own gain and may cause loss to both customers as well as the bank. Occasionally, internal bank employees purposefully compromise security to commit fraud (Ranjith 2019).

Online banking fraud

Online banking fraud refers to the unlawful use of a person's private information to make purchases or withdraw money from their bank account (Boutaher et al. 2020). Online banking fraud generally has the common deceptive characteristics of cybercrime perpetrated in a business relationship for personal gains. It is an act to intentionally deceive through false information, claim or the suppression of the truth (Crouhy, Galai & Wiener 2021). The literature reveals that the most common type of online fraud in the banking sector is phishing. Generally, phishing could be defined as a scalable act of deception whereby impersonation is used to obtain information from a victim (Arianna et al. 2022). Phishing is a form of social engineering in which a fraudster attempts to fraudulently retrieve legitimate users' confidential credentials by mimicking electronic communications or phone calls from a trustworthy or public organisation in an automated fashion (Alkhalil et al. 2021).

Figure 3 illustrate a perfect example of a phishing attack, whereby a user receives an email seeming to be from a trusted and reliable website (Sharma, Dash & Ansari 2022). The email may also contain a link that requests customers to retain their credential information and other sensitive data. When a customer enters their information, that action provides the attacker access to that information for whatever purpose they choose (Basit et al. 2021).



Source: Sharma, P., Dash, B. & Ansari, M.F., 2022, 'Anti-phishing techniques – A review of Cyber Defense Mechanisms', *IJARCCE* 11(7), 153–160

FIGURE 3: The phishing cycle.

Customers are thus never able to recognise when a phishing assault has occurred. When a customer is unaware of the attack, serios consequences could arise, including the possibility of losing valuable information permanently (Jain & Gupta 2022).

Research methods and design

Design Science Research methodology was adopted to elicit the problems and challenges of online fraud detection in the banking sector. Design Science Research is a method of research utilised to creating inventive concepts calculated to resolve everyday issues and, thus, to further the theory of the field where it is utilised (Lukka 2003). The study selected the DSR methodology as an appropriate method because the

primary key of the study is to develop a new artefact, which is a conceptual evaluation model for online fraud detection in the banking sector. Moreover, the DSR is a research method for producing innovative artefact intended to solve problems faced in the real world and, by that means, to make a contribution to the theory of the discipline in which it is applied (Lukka 2003).

Data collection methods

The study followed the qualitative research data collection approach based on the methodology implied, particularly using focus group and semi-structured interviews. The study used a focus group approach to collect data using an online platform. The focus group has its origins of group interviewing discussions as described by Merton (1956); however since then, it has gained increasing popularity within qualitative research and evaluation. With the change of times, Gundumogula (2020) stated that focus group has a way of conducting group interview discussions by using an online platform. The study used an online platform – MS Teams – to conduct interviews with participants. The online interviews were convenient and cost-effective as no traveling was required. The interview sessions were recorded, and this helped replay the recording for data analysis purposes. The focus group sessions were conducted with South African participants. A total of 17 participants were interviewed, which consisted of fraud technical managers, fraud investigator specialists, fraud technical specialist and data scientists and/or analysts from the different banking sectors.

The semi-structured interview is outlined by Gall and Gall (2003) to rely entirely on the spontaneous generation of questions in a natural interaction, typically one that occurs as part of ongoing participant observation fieldwork. Because of the complex nature of the DSR methodology, the study conducted several semi-structured interviews with Spanish fraud experts. Semi-structured interviews offered a flexible approach to data collection, where most questions came up naturally as the interview proceeded (Turner 2010).

Sampling

Sampling is an illustrative part of the targeted population that is systematically designated to participate in a research study (Rule & John 2011). The study followed non-probability samplings as it focussed on a specialised area of online fraud. Suitable participants who possess knowledge of online fraud detection models were interviewed to acquire information about the objectives of the study. The study sampled amalgamated banks of South Africa. The banking sector selection criteria was based on the results of the study found in the South African Journal of Economic and Management Sciences, which indicated an analysis of competition, efficiency and soundness of the South African banking sector (Moyo 2018). In addition, these institutions were selected because they are among the five largest banks in South Africa and have the latest technological fraud models.

Data analysis

The Atlas.ti 23 software (Jörg Hecker, Kreuzberg, Berlin, Germany) was used to support the adopted thematic data analysis process. The study followed a six-phase guide provided by Braun and Clarke (2006). The thematic data analysis helped to present qualitative data into meaningful information because the researcher was able to extract rich sets of data and described events as they occurred in a natural setting.

Ethical considerations

In order to gain access to, and acceptance in the research space, the study followed protocol as prescribed by the Tshwane University of Technology (TUT) (De Gruchy & Holness 2007). The researcher received a written approval to proceed with the study from the TUT faculty committee for research ethics (refence number: FCRE/ICT/2022/05/002(01)). Participants were issued with information consent, which included the introduction of the study, the nature, conduct and benefits. Each participant was requested to sign the consent form.

Discussions of findings

The study focussed on a specialised area of online banking fraud; suitable participants who possess knowledge of online fraud detection models were interviewed to acquire information about issues experienced in this area. The interviewee participants had different backgrounds and worked in different areas in the banking fraud department. The reason for selecting participants from different backgrounds was to obtain a holistic range of knowledge overview of the online fraud detection models. The participants consisted of fraud technical managers, fraud investigator specialists, fraud technical specialists and data scientists and/or analysts. The main issues identified by South African participants included lack of fraud experts and weak detection systems. From the Spanish perspective, the main issues included lack of customer education and lack of law regulation. The main common issue identified by both nations is social engineering. Figure 4 illustrates the identified issues from both nations.

Issues from the South African perspective

Lack of fraud experts

The findings reveal that most South African banking institutions lack online fraud experts. It was discovered that because of the high level of security provision of online fraud detection models, fraudsters have sometimes taken

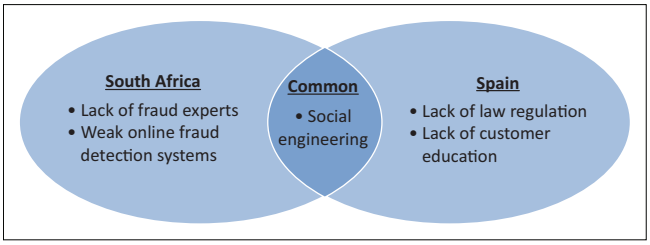


FIGURE 4: Comparison of issues identified in South Africa and Spain (Researcher).

advantage of the negligence and inexperienced online fraud experts:

> 'In one or two occasions, newly recruited staff has been deceived to disclose some vital customer' details.' (theme 1, page 112, Bank 2 transcripts)

> 'In some other occasions dubious and questionable transactions have passed through the security checks unnoticed by some newly recruited bank staff.' (theme 1, page 114, Bank 2 transcripts)

In addition, in some cases, the study revealed that some fraudulent cases occurred because of the carelessness of systems implemented by newly recruited online fraud employees. This experience has highlighted the need to acquire experienced fraud experts to protect the online fraud system and customer's confidentiality:

> 'Our main focus is therefore to protect customers' confidential information and keep the trust of our customers who can on the other hand deal with issues of identity theft or any other online fraud on their own.' (theme 2, page 133, Bank 1 transcripts)

Weak online fraud detection system

The study revealed that because of the lack of online fraud experts, the security of the detection systems is compromised. As a result, the number of increases in online fraud has been increasing every year. The evidence of an increasing number in fraud was also supported by the annual report published publicly by the South African Banking Risk Information Centre (SABRIC 2021):

> 'The rise in banking application fraud and losses can be attributed to the increased number of banking application users. The average financial loss per incident went from R12 315 in 2020, to R17 775 reported in 2021, which is a rise of 44.%.' (theme 7, page 12, SABRIC Fraud stats latest 1)

> 'In 2021 there was a 13% rise in reported fraud incidents on banking applications which increased from 10 667 cases in 2020, to 12 095 in 2021. This means that almost 42%, the bulk of digital banking crimes occurred in this segment and as a result, saw the greatest portion of gross losses at 49%.' (theme 7, page 12, SABRIC Fraud stats latest 1)

Some participants feel that the implemented fraud detection systems do not provide maximum security. Some of the weak fraud detection systems are because of legacy systems, these are systems that are very old and outdated. Banks need to upgrade to newer systems as technology advances:

> 'My feeling is that bank fraud is still a good business for fraudsters. Banks are very interested in having their customers using online banking, but they do not provide the means to maximise the security of these transactions.' (theme 5, page 46, Mariano UPV)

> '[*N*]o system is perfect. They all have their issues, whatever the issue is, it can be many things. It can be data today especially if you never had the data before you. You need it. Tomorrow it can be many customers are doing something similar to what the fraudster is doing, so it really becomes an issue to how you take something in a needle-niece type of scenario.' (theme 1, page 65, Bank 2 transcripts)

Issues from Spain's perspective

Lack of customer education

The findings revealed that some fraudulent crime occurs because of customers using the same password on their online platforms. Participants feel it is not a good practice to use the same password across that is emails, social media, online banking, among others:

> 'Research has shown then at least 70% to 80% of customers or people use the same password on Netflix, Facebook, WhatsApp, and so on and so forth as they use on their banking profile so it's very easy for fraudsters to use malware or harvest data from these various environments in order to connect the fraud so that's a big challenge we need to make sure that we continuously educate clients on how to use stronger authentication and how to make sure they use strong passwords not to kind of you know to share information.' (theme 2, page 160, Bank 1 transcripts)

> 'Although fraudsters obtained their victims' private information through social engineering techniques, they also exploited vulnerabilities in the management of critical data, and sourced usernames and passwords saved on various devices or multiple applications.' (theme 7, page 12, SABRIC Fraud stats latest 1)

This suggests that there is a lack of customer education in password etiquette; banks may be required to educate customers to create strong authenticated password for accessing online banking applications, which should be updated regularly. This will make it tough for fraudsters to gate-crash online banking systems. Banks should provide education to customers to ensure maximised security when accessing online banking applications. However, some participants indicated that it is also the responsibility of a customer to ensure they are more vigilant when making online transactions.

Lack of law regulation

The study revealed that most Spanish banking online fraud detection systems are not regulated, and this poses a high risk. Participants indicated that online banking technology is developing more rapidly than traditional transactions, and this technological advance is not only susceptible but may exacerbate and pose among others governance, legal, operational and reputational risks:

> 'This is a serious error resulting from the policies of short-term benefits.' (theme 5, page 49, Mariano UPV)

> 'There is lack of law regulation in the fraud detection systems, and also lack of collaboration between banks, it should be regulated but its not.' (theme 5, page 50, Mariano UPV)

> 'If there is a little fraud success, a big fraud success is possible. Serious enough to be the cause of a bank failure due to lack of law regulation.' (theme 5, page 51, Mariano UPV)

However, some participants mentioned that regulatory policies are there; however, they need to be updated to keep up with these technological changes, the ones that are currently in place are outdated.

Common issues to both nations

Social engineering

The most common issue identified by both nations was social engineering. Social engineering methods, such as phishing, vishing, smishing, email hacking and business email breach, were prevalent and the most main ways that people committed fraud in online banking. Fraudsters frequently call victims, impersonate a bank official and then use social engineering skills to manipulate the victim into disclosing private information that is then used to defraud them:

> '[*F*]raudsters normally gather data through social engineering so they harvest data through social network like Facebook and Instagram etcetera because people say a lot of things on social network profile.' (theme 2, page 123, Bank 1 transcripts)

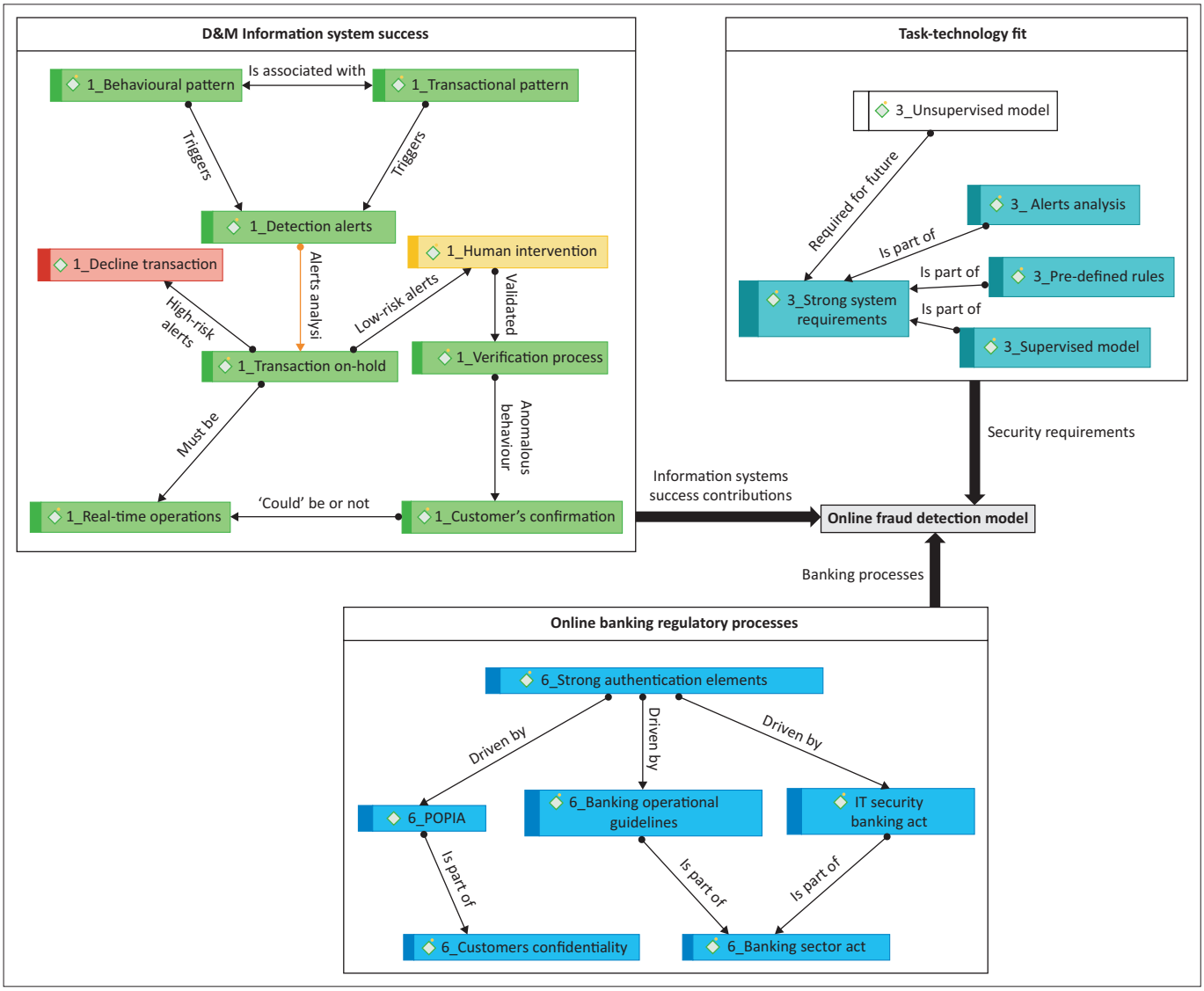
> 'A lot however depends on the ignorance of the people which is often exploited by fraudsters. These ignorant people in most cases ignorantly help the fraudsters by exposing their information on social media.' (theme 2, page 125, Bank 1 transcripts)

> 'Social engineering techniques including, but not limited to phishing, vishing, smishing, email hacking and business email compromise continued to prevail and were the most prominent fraud methods in the digital banking fraud space T.' (theme 7, page 12, SABRIC Fraud stats latest 1)

The findings show that online fraud is still on the increase because of the ignorance of most customers and online users. Participants highlighted that the ignorance of most customers is caused by users who disclose their personal information on social media. Fraudsters normally gather data through social networks like Facebook and Instagram because people usually mention a lot of things on these platforms. Bank customers need to be vigilant about what information they say on social media.

Artefact

The study developed an artefact for the online fraud detection model using the DSR cycles (Wieringa 2014). The first cycle was conducted to establish problems awareness. The second cycle mainly focussed on the development of a conceptual model. The third cycle predominantly concentrated on the



D&M, DeLone and McLean; POPIA, Protection of Personal Information Act.

FIGURE 5: Conceptual model for online fraud detection in the banking sector (Researcher).

evaluation of a conceptual model. The DSR methodology was the most appropriate approach because it allowed the study to enhance knowledge bases in online banking fraud through the creation of the conceptual model. The final artefact implemented is shown in Figure 5.

Conclusion

The main objective of the study was to investigate issues of online fraud detection in the banking sector in cases from South Africa and Spain. The objective of the study was achieved by gathering relevant data from online fraud experts working in the banking sector from both nations. Their experience, expertise and knowledge contributed to identifying the online fraud issues at hand. The study fulfilled the objective by using the DSR methodology. This methodology was the most appropriate approach because it allowed the study to enhance knowledge in this subject matter. The study revealed that there is a lack of online fraud expertise in South Africa, and this may lead into banks having weak detection systems. Therefore, it is suggested that the South African banking sector needs to train more employees in this area. Experienced fraud expertise may help to build stronger detection systems to combat online banking fraud. From Spain's perspective, the main findings were about lack of regulation. These findings suggest that regulators are required to consistently update the online banking process to keep up with the technological developments. As highlighted in previous studies, this study expands limited theory on online banking fraud both in the banking sector and academia.

Limitations

The study suffered because of a lack of prior research in online fraud contexts both from South Africa and Spain, which would have laid the foundation for understanding the issues investigated. The sample size was not large enough to be representative of a large population because of the qualitative research method used. A large sample size would have been achieved if a quantitative research method was used. The study depended on having access to the online fraud experts; the researcher could not access some of the data required to accomplish the study because of sensitive data held by the banking sector.

Recommendation

The study will be a significant contribution to the topic of online banking fraud in the banking sector and within academia as few studies were found during the literature review. The issues identified by the study are recommended to be used as a guideline when developing new practical online fraud detection solutions for the banking sector in the future. The scarcity of online banking fraud studies was also mentioned by the fraud experts and participants during data collection; therefore, it is recommended that further research on this topic be executed in the future. Further research will be a considerable contribution as it will add new knowledge to the area of study about online banking fraud. The DSR methodology is not only useful in the research of online banking fraud but also it could be beneficial in any other areas of research.

Acknowledgements

I would like to thank my supervisors and all the participants who contributed excellently to the success of the article.

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

Authors' contributions

J.P. was the main author of the article and conducted most of the research, while T.J.L. was the co-author performing the main supervisory role and M.A.S. provided co-supervising support.

Funding information

The study was partially funded by the Erasmus+ KA107 student mobility project under the partnership between Universitat Politecnica de Valencia, Spain and Tshwane University of Technology, South Africa.

Data availability

The data that support the findings are available on request from the corresponding author, J.P.

Disclaimer

The views and opinions expressed in this article are those of the authors and are the product of professional research. It does not necessarily reflect the official policy or position of any affiliated institution, funder, agency, or that of the publisher. The authors are responsible for this article's results, findings, and content.

References

Alkhalil, Z., Hewage, C., Nawaf, L. & Khan, I., 2021, 'Phishing attacks: A recent comprehensive study and a new anatomy', *Frontiers in Computer Science* 3, 563060. https://doi.org/10.3389/fcomp.2021.563060

Arianna, T., Kamps, J., Akartuna, E.A., Hetzel, F.J., Bennett, K., Davies, T. et al., 2022, 'Cryptocurrencies and future financial crime', *Crime Science* 11, 1. https://doi.org/10.1186/s40163-021-00163-8

Balasupramanian, N., Ephrem, B.G. & Al-Barwani, I.S., 2017, 'User pattern based online fraud detection and prevention using big data analytics and self organizing maps', in *2017 international conference on intelligent computing, instrumentation and control technologies (ICICICT)*, IEEE, Kerela, India, July 06–07, 2017, pp. 691–691.

Basit, A., Zafar, M., Liu, X., Javed, A.R., Jalil, Z. & Kifayat, K., 2021, 'A comprehensive survey of AI-enabled phishing attacks detection techniques', *Telecommunication Systems* 76, 139–154. https://doi.org/10.1007/s11235-020-00733-2

Boutaher, N., Elomri, A., Abghour, N., Moussaid, K. & Rida, M., 2020, 'A review of credit card fraud detection using machine learning techniques', in *2020 5th international conference on cloud computing and artificial intelligence: Technologies and applications (CloudTech)*, IEEE, Marrakesh, Morocco, November 24–26, 2020, pp. 1–5.

Braun, V. & Clarke, V., 2006, 'Using thematic analysis in psychology', *Qualitative Research in Psychology* 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Carneiro, N., Figueira, G. & Costa, M., 2017, 'A data mining based system for credit-card fraud detection in e-tail', *Decision Support Systems* 95, 91–101. https://doi.org/10.1016/j.dss.2017.01.002

Crouhy, M., Galai, D. & Wiener, Z., 2021, 'The impact of fintechs on financial intermediation: A functional approach', *The Journal of FinTech* 1(01), 2031001. https://doi.org/10.1142/S270510992031001X

Daliri, S., 2020, 'Using harmony search algorithm in neural networks to improve fraud detection in banking system', *Computational Intelligence and Neuroscience* 2020, 6503459. https://doi.org/10.1155/2020/6503459

Damrongsakmethee, T. & Neagoe, V.-E., 2017, 'Data mining and machine learning for financial analysis', *Indian Journal of Science and Technology* 10(39), 1–7. https://doi.org/10.17485/ijst/2017/v10i39/119861

De Gruchy, J.W. & Holness, L., 2007, *The emerging researcher: Nurturing passion, developing skills, producing output*, Juta and Company Ltd., Cape Town.

Gall, G., Borg, W.R. & Gall, J.P., 2003 , *Educational research: An introduction*, 7th edn., Longman, New York, NY.

Gregor, S. & Hevner, A.R., 2013, 'Positioning and presenting design science research for maximum impact', *MIS Quarterly* 37(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01

Gundumogula, M., 2020, 'Importance of focus groups in qualitative research', *The International Journal of Humanities & Social Studies* 8(11), 299–302. https://doi.org/10.24940/theijhss/2020/v8/i11/HS2011-082

Jain, A.K. & Gupta, B., 2022, 'A survey of phishing attack techniques, defence mechanisms and open research challenges', *Enterprise Information Systems* 16(4), 527–565. https://doi.org/10.1080/17517575.2021.1896786

John, S.N., Anele, C., Kennedy, O.O., Olajide, F. & Kennedy, C.G., 2016, 'Realtime fraud detection in the banking sector using data mining techniques/algorithm', in *2016 international conference on computational science and computational intelligence (CSCI)*, IEEE, Las Vegas, NV, December 15–17, 2016, pp. 1186–1191.

Krishnan, J.M., 2017, 'Customers attitude towards e-banking system in Chennai', *International Journal of Research in Management & Social Science* 5(3), 68.

Kumar, M.D., Mubarak, A. & Dhanush, M., 2020, 'Credit card fraud detection using Bayesian belief network', *International Journal of Research in Engineering, Science and Management* 3(7), 316–319.

Lukka, K., 2003, 'The constructive research approach', *Case Sresearch in Logistics* 1, 83–101.

Merton, R.K., 1956, *The focussed interview: A manual of problems and procedures, by Robert K. Merton, Marjorie Fiske [and] Patricia L. Kendall*, Free Press, New York, NY.

Minastireanu, E.-A. & Mesnita, G., 2019, 'An analysis of the most used machine learning algorithms for online fraud detection', *Informatica Economica* 23(1), 5–16. https://doi.org/10.12948/issn14531305/23.1.2019.01

Moyo, B., 2018, 'An analysis of competition, efficiency and soundness in the South African banking sector', *South African Journal of Economic and Management Sciences* 21(1), 1–14. https://doi.org/10.4102/sajems.v21i1.2291

Rahi, S. & Abd. Ghani, M., 2019, 'Investigating the role of UTAUT and e-service quality in internet banking adoption setting', *The TQM Journal* 31(3), 491–506. https://doi.org/10.1108/TQM-02-2018-0018

Ranjith, S., 2019, 'Growth of e-banking: Challenges and opportunities in India', *SELP Journal of Social Science* X(40), 50, 54.

Raza, S.A., Umer, A., Qureshi, M.A. & Dahri, A.S., 2020, 'Internet banking service quality, e-customer satisfaction and loyalty: The modified e-SERVQUAL model', *The TQM Journal* 32(6), 1443–1466. https://doi.org/10.1108/TQM-02-2020-0019

Rule, P. & John, V., 2011, *Your guide to case study research*, van Schaik, Pretoria.

SABRIC, 2021, *Annual crime statistics 2021*, p. 1, viewed n.d., from www.sabric.com.

Shankar, A. & Rishi, B., 2020, 'Convenience matter in mobile banking adoption intention?', *Australasian Marketing Journal* 28(4), 273–285. https://doi.org/10.1016/j.ausmj.2020.06.008

Sharma, P., Dash, B. & Ansari, M.F., 2022, 'Anti-phishing techniques – A review of Cyber Defense Mechanisms', *International Journal of Advanced Research in Computer and Communication Engineering* 11(7), 153–160. https://doi.org/10.17148/IJARCCE.2022.11728

Singla, A. & Jangir, H., 2020, 'A comparative approach to predictive analytics with machine learning for fraud detection of realtime financial data', *2020 international conference on emerging trends in communication, control and computing (ICONC3)*, IEEE, Lakshmangarh, India, February 21–22 2020, pp. 1–4.

Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S. & Kuruwitaarachchi, N., 2019, 'Real-time credit card fraud detection using machine learning', *2019 9th international conference on cloud computing, data science & engineering (confluence)*, IEEE, Noida, India, January 10–11, 2019, pp. 488–493.

Turner III, D.W., 2010, 'Qualitative interview design: A practical guide for novice investigators', *The Qualitative Report* 15(3), 754.

Wieringa, R.J., 2014, *Design science methodology for information systems and software engineering*, Springer, London.