Fraud Detection System Adoption: Success Factors

Mehmet Akgul
McMaster University, akgulm.ca@gmail.com

Follow this and additional works at: https://aisel.aisnet.org/ecis2021_rip

Recommended Citation
https://aisel.aisnet.org/ecis2021_rip/50

This material is brought to you by the ECIS 2021 Proceedings at AIS Electronic Library (AISeL). It has been accepted for inclusion in ECIS 2021 Research-in-Progress Papers by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
FRAUD DETECTION SYSTEM ADOPTION: SUCCESS FACTORS

Research in Progress
Mehmet Akgul
McMaster University
akgulm@mcmaster.ca

Abstract
Failure to prevent and detect fraud has severe consequences for organizations. Organizations confront not only monetary losses but also reputation and customer trust. Fraud detection is a complex task and incorporates many mechanisms. While the risk of fraud cannot be completely eliminated, it may be reduced by using multiple mechanisms such as technological platforms, internal controls, and regulatory requirements. Combating fraud can be done in a two-consecutive process, namely fraud prevention and detection. In this study, by utilizing the Technology–Organization–Environment Framework (TOE), we have identified the factors affecting fraud detection system adoption. Such understanding may bring new insights to the discussion and provide contributions to both practitioners and researchers alike.

Keywords: Fraud Detection, System Adoption, TOE Framework

1 Introduction
Association of Certified Fraud Examiners (ACFE) defines fraud as “fraud includes any intentional or deliberate act to deprive another of property or money by guile, deception, or other unfair means (ACFE, n.d.)”. Due to fraud, organizations face not only financial losses but also reputation and trust. As Experian (2016) asserted, the cost of fraud to the UK is as much as £193 billion per year. According to the Association of Certified Fraud Examiners (ACFE, 2016a), each year, a typical organization loses 5% of its revenue to occupational (internal) fraud, where 23% of the losses are above $1 million. As Everest Group (2014) stated, financial institutions do not face just financial losses but also customer trust and, thus, customer loyalty. To not lose customers, some organizations do not even announce fraud cases to the public. ACFE (2016b) reports that 40% of fraud cases are not reported to law enforcement.

There are numerous ways of classifying fraud. Bologna and Lindquist (1995) classified the fraud whether the perpetrator is internal or external to the victim company. A combination of internal and external fraud can also happen when an employee collaborates with an external entity (Jans et al., 2010). According to Mufutau and Mojisola (2016), people ask three questions to themselves before committing fraud: "Is it more than the job is worth? Will I get caught? and Is it right or wrong?” After considering these questions, people decide to commit fraud or not.

Based on the industry, fraud cases may be further classified, such as financial (bank and insurance) fraud, telecommunications fraud, healthcare fraud and e-commerce fraud. Some of the examples of fraud in different industries are as follows (Baesens et al., 2015): Opening new bank accounts using a victim’s information without his knowledge and permission (Banking), Invoicing for the services that are not taken (Healthcare), selling services that do not exist (Insurance)

According to Cressey (1953), fraud occurs when there is an incentive to commit fraud, a rationalization for justifying fraudulent behaviour and an opportunity to commit fraud. Due to its
importance, many organizations, especially the financial sector, use different mechanisms to combat fraud. Combating fraud can be done in a two-level process where the first step is the prevention step, and the second one is the detection step (Behdad et al., 2012).

Fraud prevention refers to all the actions that stop fraud from happening. Fraud detection is composed of all mechanisms, both technological and human activities, to detect fraud once it occurs. While in fraud prevention, the aim is to stop the fraud, the objective of fraud detection is to minimize the cost of the fraud (Kou et al., 2004).

Due to its importance, it is crucial to understand the factors affecting the adoption of Fraud Detection Systems (FDSs). Although there are some studies that explored the adoption of Information Security Solutions (ISSs)( Herath et al. 2020; Hasan et al., 2021) FDSs are different than the ISSs in the sense that FDSs are being used to protect the clients of the organization, e.g. bank account holders, not the organization itself. Thus, the purpose of this paper is to identify the factors that explain the FDS adoption. Specifically, by adopting the Technology–Organization–Environment Framework (TOE) as the basis, we investigated the following research question: "What are the organizational, technological, and environmental factors in the Fraud Detection System adoption?". We are interested in the transactional FDSs where customers’ transactions are already available to the organization. To the best of our knowledge, this paper is one of the first studies that examine FDS adoption.

2 Literature Review

2.1 Technological Challenges in Fraud Detection

FDSs are being used in the industry for detecting various fraud cases. Depending on the industry and organizational capability, these systems can work online, i.e. real-time or offline. In an online system, the transaction is fed into the FDS, and the response is obtained within a short period, e.g. in milliseconds. In an offline system, the transactions are supplied to the FDS, but the response is received after hours or days. While online banking transactions are screened in real-time for fraud detection, anti-money laundering checks are done offline to the authors' knowledge.

Generally, FDS tools are divided into two categories: static rule engines and data mining supported engines (Quah & Sriganesh, 2008). However, some of the FDS tools offer both of the functionalities together. Depending on the industry, various rule-based engines are being used (Rosset et al., 1999). A rule-based engine consists of if-then rules and provides output from a set of options that are given facts (Abraham, 2005). As an example, some banks screen transactions in real-time for specific people or locations and block the transactions if the person or place is on the bank's blacklist (Muir & Oorschot, 2006). In telecommunications, Moreau et al. (1996) proposed a rule-based fraud detection system where the system compares the average number and duration of predefined call properties, e.g. international calls, against user-defined threshold values. From a human resources perspective, such platforms' maintenance cost is low (Mongeau, 2014).

Data mining supported FDS tools use various data mining methods to detect fraudulent transactions. From the data mining perspective, fraud detection is a classification problem where the transactions are classified as either legitimate or fraudulent. Depending on the industry and the data mining problem, e.g. classification, clustering or outlier detection, various data mining methods such as logistic regression, probit regression, decision trees, random forests, support vector machines, fuzzy systems, genetic algorithms, artificial neural networks and Bayesian belief networks are being developed for fraud detection (Sahin and Duman, 2011; Francis et al. 2011; Dunn and Kim, 1999; Liu et al., 2015; Bhowmik, 2008; Bentley et al., 2000).

FDS solutions can either provide the transaction class (legit or fraudulent) or the probability of the transaction being a fraudulent one. With cloud computing, some scholars proposed or developed fraud detection engines running on the cloud (Halvaeie & Akbari, 2014; Unal & Yates, 2010; Hormozi et al., 2013).
Although static rules are easy to implement and interpret, one of the difficulties in developing rules is domain expertise. Thus the rules are as successful as the knowledge of the domain expert. If the domain expert does not know a fraud pattern, he cannot develop a rule for that kind of fraud. This issue can be partially be solved using industry-wide FDS solutions since that kind of solution contains the expertise gained through working with multiple organizations.

However, static rule-based solutions do not eliminate fraud since fraudsters may learn the fraud detection rules and may change their transaction pattern to circumvent those engines. For example, in smurfing, a type of money laundering, the person divided the total money into small accounts to not file a currency transaction report required by authorities for any cash transactions exceeding $10,000 (Takáts, 2009). Static rules in this kind of incident may not catch the fraudsters.

The application of data mining methods may eliminate some of the drawbacks of the use of static methods. However, data mining methods are not perfect in their tasks. For example, the success of Support Vector Machines (SVM) used for credit card fraud detection (Şahin & Duman, 2011; Chen et al., 2005) depends on the training data, transaction features included in the data, the kernel method and its parameters. Moreover, SVM classifies a transaction either as legitimate or fraudulent but does not justify the decision. Such difficulties also exist for other data mining methods. For example, e.g. selection of node division methods in decision trees and the number of hidden layers and activation methods in neural networks significantly affect their success level.

Another method that was proposed for fraud detection is outlier detection. According to Agyemang et al. (2006), an outlier in a dataset is a data point whose characteristics are different from the other data points. However, what may be an outlier in one situation may be completely normal in another case. As pointed by Rosset et al. (1999) in telecommunications, a Premium Rate Service call may be typical if the customer usually makes such calls, but suspicious if it is not the case. Due to its definition, i.e. difference, many methods were proposed for outlier detection (Agyemang et al., 2006). Hodge and Austin (2004) further pointed out that no generic outlier detection method and the selection method depend on the data and the problem.

To eliminate some of the difficulties stated above, some authors proposed to use an ensemble of data mining methods in fraud detection (Phua et al., 2010). Although such applications may increase the accuracy of fraud detection, they also increase the system's complexity. Compared to the static rule engines, data mining supported FDSs to detect fraud (Mongeau, 2014) effectively. However, as the author claims, they are also more costly than static rule engines. We believe that this is because data mining methods require specialized knowledge. Another challenge that should be considered in the application of data-mining techniques is that they should regularly be adjusted as the success of the data mining methods depends on the data, i.e. good users' and fraudsters' transactions' pattern, and the parameters of the method itself (Bolton & Hand, 2002; Lei & Ghorbani, 2012).

Lack of publicly available data is also another challenge for fraud detection. Since fraud is sensitive due to financial, privacy-related or legal reasons, publicly available data is scarce, and organizations tend to use in-house solutions for fraud detection (Lopez-Rojas et al., 2013). This makes it hard to develop effective fraud detection systems, even in the same industry. Although organizations can use industry-wide FDS solutions, those solutions have only standard static rules, and the bought solution should be trained using the organization's data itself since the organization's fraud cases are specific to that organization.

The fraud incident distribution also makes it harder to distinguish a fraudulent transaction from a legitimate one, indeed. Although there are many fraud cases, the percentage of fraud incidents is very low compared to legitimate transactions (Gadi et al., 2008). Such skewness of the fraud data brings in additional difficulty in the accuracy of the data mining methods, and it may be the case that such methods may predict all transactions as legitimate and miss fraudulent ones (Lei & Ghorbani, 2012).

Another challenge for fraud detection systems is the high volume of transactions. Recent technological developments, e.g. spread of the internet, web and mobile-based applications, enabled people to make transactions easily. Processing such an amount of transactions requires effective and efficient methods and underlying infrastructure. To accommodate such a high volume of transactions, Kavitha and
Suriakala (2015) suggested using either GPUs (graphics processing unit), due to their high processing power or big data platforms such as Hadoop. However, GPUs have been designed entirely differently from CPU (central processing units), and GPUs' use requires either new implementations of the current algorithms or the development of new algorithms tailored to their design.

Compared to external fraud, detection of fraud done by internal employees is more challenging. This so since internal employees may know the weak points in fraud detection. As reported by Adamson (2017), a bank teller stole $1.25 Million over ten years. The FDS tools could not detect the fraud since she falsified the entries taking small denominations every day. The fraud was discovered after careful investigation of the account books done since another institution bought the bank. Also, since bank employees can reach the clients' accounts, they may make unauthorized withdrawals and deposits. The employee first withdraws money from the account, then uses it for his own purposes, e.g. in the stock market, and then deposits the money back to the account. Such transactions cannot be detected unless the account holder notifies the bank. This is because such transactions are claimed to be done by order of the customer. In the past, some of the fraudsters were catches for committing this kind of fraud (Adamson, 2017; Clarke, 2016).

Both data mining and rule-based methods can be used in fraud detection if the transaction is highly structured. In some industries, e.g. healthcare, the transactions, e.g. doctor visits, do not have a structure. According to Kim et al. (2014), approximately 90% of the generated data in organizations is unstructured. Whereas structured data can be easily stored, queried, and analyzed by a machine, it is not the case for unstructured data since it contains handwritten notes, different kinds of images, or audio or video files. Thus, effective and efficient technological solutions should be developed to analyze unstructured data, especially healthcare (Raghupathi & Raghupathi, 2014).

### 2.2 Organizational Challenges in Fraud Detection

Due to the sensitivity of the issue, fraud-related decisions cannot be made by the FDS tools' outputs. Thus, in addition to using technological platforms, organizations should also provide necessary fraud detection mechanisms. Within this section, we will address some of the challenges organizations face during the fraud detection process.

Although technological platforms can be used in fraud detection, they cannot fully guarantee that a transaction is legitimate or fraudulent. Because of this possibility of error, those systems' output is not enough to act as legal proof. Hence a transaction or claim should be investigated carefully. Moreover, considering the situation's seriousness, some organizations take the fraud burden and pay out the claimed amount rather than making a possible faulty action (Viaene & Dedene, 2004). Therefore, the balance between detecting fraud and claiming someone as a fraudster or bearing the fraud burden should be considered by each organization separately since the amount of the fraud and the organization's financial capacity to cover it is organization-specific.

Another challenge that organizations should consider is the processing efficiency since there is a tradeoff between fraud detection and customer satisfaction (Viaene & Dedene, 2004). It may be the case that organizations may cover the cost of fraud for better customer satisfaction instead of making a lengthy fraud investigation. As stated in the previous paragraph, making an investigation or covering the cost is an organization-specific issue, and management should set the decision.

Related to the above challenges, one other challenge in fraud detection is its return on investment quantification. Measuring the value of fraud detection is not easy, and although technological platforms can be used in fraud detection, the use of such sophisticated technical solutions brings an additional cost to the organizations. Thus those solutions should be economical in combating fraud (Turney, 1995). Bhatla et al. (2003) stated that a review of 30% of transactions could reduce the fraud losses to 0.06%, but in turn, this review increases review costs enormously. Thus, the balance between the cost involved in transaction screening and review and the losses due to fraudulent cases should be taken into account by the management for fraud detection projects. According to the authors' own experiences, some banks do not deploy industry-wide used fraud detection solutions since they believe
that those solutions far exceed the cost of the fraud itself. They can implement in-house solutions if necessary.

2.3 Regulatory Challenges in Fraud Detection

Although technological platforms and internal control mechanisms can be used in fraud detection, their existence may not be sufficient for effective fraud detection. Relevant regulatory bodies should be established, auditors and investigators should be supported, and privacy concerns should be addressed during a fraud investigation. We will address some of the challenges that should be addressed by regulatory authorities in the following paragraphs.

While data analytics platforms may be used for fraud detection, they also reveal the individuals' behaviour. Therefore, privacy concerns should also be addressed during the fraud detection process. Revealing such behavioural patterns may be against the privacy laws in some countries. Furthermore, according to some privacy laws, any data should be used only for the purposes that it was collected for, and thus unauthorized data cannot be used for fraud detection purposes (Cardenas et al., 2013). This may impose an additional barrier for organizations in fraud detection. According to the authors' own experiences, to overcome this kind of difficulty, some organizations, especially those in the financial industry, get the customers' permission and employees' permission to use the data for internal purposes. However, this is still a problem for both customers and employees since they may unwillingly provide their permission. To overcome this difficulty, as asserted by Tene and Polonetsky (2012), policymakers should address the privacy law by defining the organization's roles and individuals in the collection, control, and analysis of data. Without such regulations, organizations may use data other than fraud detection purposes or fail to detect fraud if they cannot use the collected data.

It has been argued that relevant information on fraud, anti-fraud and (potential) fraudsters remain overly dispersed and under-utilized and that establishment of anti-fraud alliances composed of organizations, public authorities, and other stakeholders may facilitate the prevention, detection, investigation, and prosecution of fraud (Vianee & Dedene, 2004). Authors argue that such collaboration enables linking up and sharing detailed information related to fraud. Although there are some anti-fraud alliances for the financial sector, i.e. for banking and insurance such as OFAC, other sectors, e.g. healthcare, telecommunications or e-commerce, according to the author's best knowledge, such anti-fraud alliances do not exist. Since the financial industry is highly regulated, it might have been easier for that industry to build a shared knowledge base. However, regulatory organizations may at least provide an initiative to develop such anti-fraud alliances for other industries for combating fraud effectively.

Also, the lack of a law of the definition of fraud as a crime in some industries is another issue that should be addressed (Tennyson, 2008). According to the author, the existence of fraud-related laws increases the ability to detect fraud. Also, Vianee and Dedene (2004) suggest that related laws should be defined for fraud not only for preventing it from occurring but also for enabling auditors to make investigations without fear of being sued for invasion of privacy. However, defining fraud may not be so easy for regulatory bodies since fraud cases are continually changing, and there are various fraud cases across multiple industries.

3 Proposed Research Model and Hypotheses

Figure 1 shows the proposed research model. We selected the TOE framework (Tornatzky and Fleischer, 1990) that affects the adoption and implementation of technology (Salleh and Janczewski, 2016).
Fraud Detection System Adoption: Success Factors

TOE framework provides a holistic approach considering both internal (technology and organization) and external (environment, i.e. industry and government) factors in the technology adoption, and it has been used by many IS researchers to explain the adoption of technologies such as Electronic Data Interchange (Kuan and Chau, 2001) and Enterprise Resource Planning (Pan and Jang, 2008), e-business adoption (Tiago and Maria, 2010), cloud service adoption (Haag and Eckhardt, 2014), cyber Insurance Instruments (Bandyopadhyay, 2012) and cybersecurity readiness of organizations (Hasan et al., 2021). That is why we also believe that the TOE framework can be appropriate in our study.

Organizations should also be aware of difficulties in the implementation of technological platforms. Although using an industry-wide FDS may help organizations in fraud detection, those solutions are so generic that they have to be configured according to organization needs. Installation of such software solutions is not enough, and those solutions should be continuously monitored and updated since the user, whether good or bad, behaviour changes continuously. As implementation and maintenance of such software can be complex, the adoption of an FDS can be impacted by the ease of implementation. Hence aligned with Bach et al. (2016), we posit that

**H1: Perceived Ease of implementation positively influences FDS Adoption.**

Practitioners should also consider the amount of data and the processing speed of transactions in fraud detection. It may be the case that customer dissatisfaction may occur due to the latency of transactions. The cost of such dissatisfaction may be much more than the total fraud incidents that the organization faced. As the DeLone and McLean (2003) model of information systems success, system response time is one of the characteristics of the system quality. Hence, aligned with them, we posit that:

**H2: System response time is positively associated with FDS Adoption.**

Organizations should also consider the definition of such technological platforms' success metrics since a standard evaluation metric in fraud detection does not exist. High accuracy may not be simple enough if those solutions can only detect fraud incidents with small amounts and fail to catch those with large amounts. These definitions significantly affect the configuration and implementation, and eventually, FDSs and organizations' success should set these metrics before starting to implement such a project. As Whyte et al. (1997) suggest, "a successful information system is one which achieves the expectations of its users. (pp.38)" and the definition of success depends on organizations' own interpretations. Hence, we posit that:

**H3: Perceived system success is positively associated with FDS Adoption.**

The return on investment and customer satisfaction should also be considered by organizations while implementing those solutions. As described in the previous section, it may be the case that the cost implementation of those solutions and the investigations afterward may exceed the cost of fraud itself. Also, since it is a sensitive issue, wrongly alleging one may result in reputation issues and lawsuits. Thus organizations should find a balance between the cost of fraud and its detection. The perceived cost was found to be one of the important factors in the adoption of other information technologies such as mobile technology (Naicker & Merwe, 2018). Hence, we posit that:

**H4: Perceived system cost is positively associated with FDS Adoption.**
Due to its high regulation, well-known anti-fraud alliances exist for the financial industry. These alliances provide training to their members and provide a knowledge base where each member can both contribute and use. Such knowledge-sharing eased financial actors to detect fraud. To the author's best knowledge, for other industries, such alliances do not exist. Although such partnerships are not required for fraud detection, their inexistence may result in ineffectiveness in fraud detection (Viaene & Dedene, 2004). As Iacovou et al. (1995) suggested and Oliveira and Maria (2010), partner collaboration positively affects technology adoption. Hence, we posit that:

**H5: The existence of Anti-Fraud alliances is positively associated with FDS Adoption.**

Although more fraud data is better to understand and capture the fraud, it may also reveal personal behaviour. To ensure that there are no privacy breaches, regulatory authorities should address the privacy concerns for fraud detection, e.g. what data to collect and when and how to destroy it once it is used. However, we also believe that such fraud knowledge may also be beneficial for the scholarly world to devise better fraud detection methods and thus believe that the regulatory organizations should also address this. Governments can enhance the technology adoptions by fundings (Lawson et al., 2003) and also by also enforcing regulation compliance (Troshani et al., 2010). Hence, we posit that:

**H6: The existence of government support and regulations are positively associated with FDS Adoption.**

### 4 Proposed Methodology

An online survey will be conducted to test our research model. To test our model's robustness, we will target companies in different sectors, such as insurance, bank and retail, in at least two different counties. We will send emails to CFOs and CIOs of the target companies to complete an anonymous online survey about the organization and environment, and technology-related factors of FDS adoption. To increase the survey participation rate, we will suggest sharing the results of our analysis with the organizations, which can guide them in the enhancement/mitigation of FDS adoption factors. The operationalization of the variables and the survey questions will be taken from the extant literature. For example, *Perceived Ease of implementation* will be measured using the Likert scale items adapted from Bach et al. (2016): "Implementation process of FDS is understandable", "IT department has adequate knowledge for FDS implementation", "It is easy to integrate FDS with existing solutions" and "Company has adequate financial resources for FDS implementation". We will develop new items for the *Perceived system success* and *Perceived system cost* constructs. For *Existence of Anti-Fraud alliances* and *Existence of government support and regulations* binary variables (0/1) will be used in our study. We will conduct a regression analysis after gathering the data, and we will share our findings with the participant organizations.

### 5 Conclusion

Fraud detection is a complex task and incorporates many mechanisms. While the risk of fraud cannot be eliminated, it may be reduced by using multiple mechanisms such as technological platforms, internal controls, and regulatory requirements.

Fraud detection requires effective and efficient detection mechanisms without affecting business operations' smoothness and customer satisfaction. It is needed for security concerns and to maintain trust between the various parties, e.g. customers, organizations, and legal authorities. The loss of trust between parties may result in substantial economic losses. By using the TOE framework, this study tried to explain the factors in the adoption of Fraud Detection Systems. This paper does not claim to be exhaustive, but to the best of our knowledge, this study is one of the few studies investigating the factors in the adoption of FDSs.
References


Amaya de la Pena, I. (2017). Fraud detection in online payments using Spark ML: Master thesis performed in collaboration with Qliro AB.


