Electronic Journal of Business and Management
Vol.6 Issue 2, 2021 pp. 18-29
e-ISSN:2550-1380-ISSN

THE ESSENCE OF CYBERSECURITY THROUGH FINTECH 3.5 IN PREVENTING AND DETECTING FINANCIAL FRAUD: A LITERATURE REVIEW

Nagasundari A/P Selvaraj
Asia Pacific University of Technology and Innovation
TP061219@mail.apu.edu.my

Abstract

The dramatic upsurge in cybercrime demands the need of effective security measures that ensures safety in cyberspace. With the development of Fintech 3.5, the role of effective cybersecurity has gained significant attention among the users of Internet, which includes both groups of users with harmless and malicious intentions. The increase in reliance of cyberspace for daily transactions and activities such as investments, money exchanges and online purchases have caused cyber-attacks to be in its peak, as no industries or organisations can be bulletproof when it comes to cyber threats. Therefore, this paper aims to explore the role of cybersecurity, which is aided by Artificial Intelligence (AI) in preventing and detecting financial fraud. The highlight of this paper surrounds the comprehension of cybersecurity, encompassing its tools, applications, challenges, and regulatory conditions that influences its function. The concept of cybersecurity is of compelling requirement, thus resulting prominence in this literature review to contribute as a foundation for the complex IoT environment that is engaged by users. Future areas to be explored under this context have also been discussed in this paper.

Keywords: *Cybercrime, Fintech 3.5, Financial Fraud, Artificial Intelligence, Cybersecurity, Tools, Challenges, Regulation*

1.0 Introduction

The usage of modern technologies has now become embedded in the lives of all individuals, connecting people and businesses worldwide with no geographical boundaries. The concept of Fintech is no stranger to the modern world, being the backbone of contemporary finance in processing simple automation to complex cognitive decision making and analytics (Knewtson and Rosenbaum, 2020). The evolution of Fintech commenced with Fintech 1.0, in an effort to incorporate finance with technology to achieve financial globalisation through the emergence of Diners Club (Das, 2019; Nasir and Saeedi, 2019). Later, Fintech explored the digital world to cater for better communication and transactions, in which ATMs, NASDAQ and SWIFT were established through Fintech 2.0. Public perception, economic conditions and the regulatory compliance have further developed Fintech into the third phase of Fintech 3.0, through the introduction of Bitcoin and Blockchain. Due to the rapid growth in economy and e-commerce, the need for secured digital transactions and the demand for powerful data security have transformed into Fintech 3.5, which is now the spotlight of Fintech venture

(Arner, Barberis and Buckley, 2015). Being in the bleeding edge of technology, the advancement comes with a threat of security, which hinders the usefulness of Fintech through financial fraud such as illegal hacking into banking system, unauthorised network access and money laundering. Cyberthreat Defence Report of 2020 reveals that the finance industry has the highest percentage of cyberattack in the past 12 months, recording 87.6% (Cyber Egde Group, 2020). The facility of Internet has made traditional financial fraud to be more complex and challenging as the concept of anonymity makes it complicated to trace cybercriminals with obsolete or basic technologies. Hence, the role of cybersecurity in the modern computer era is in the limelight for preventing and detecting financial fraud. With the increasing reliance on cybersecurity to protect data and to induce a safe financing environment, the government regulations surrounding the area of cyber law is substantial in assuring integrity of transactions occurring in cyberspace. Thus, this paper aims to venture into the aspect of cybersecurity in preventing and detecting financial fraud, enclosing the cybercrime platforms, tools and applications of cybersecurity, the regulatory environment, and the challenges of implementing cybersecurity solutions.

2.0 The Emergence of Fintech 3.5

As globalisation and digitalisation began to take centre stage, financial services were revolutionised, by which various startups and large organizations launched online platforms to perform financial transactions. The stereotype boundaries for regulated financial institutions were defeated with the emergence of Fintech 3.0, which was the foundation for the emergence of Fintech 3.5 (Setiawan and Maulisa, 2020). The deviation from traditional banking system and the introduction of modern technologies such as Bitcoin and digital wallets had paved a way to an improved industry of Fintech 3.5. The major difference between both the eras lies in the state of economy the users are experiencing (Arner, Barberis and Buckley, 2015). Developed countries with greater level of banking infrastructure and network distribution have adopted Fintech 3.0.

On the other hand, developing countries in the Asia-Pacific region, which have lagged infrastructure development and less competitive market have leveraged on the alternative solutions for their financial needs, thus, have an extensive reliance on technology, prompting the evolution of Fintech 3.5. This is evidenced through the report of Global FinTech Adoption Index 2019, that states the adoption rate of Fintech in China, India and South Africa are 87%, 87% and 82% respectively (Ernst & Young, 2019). These emerging markets are leading the FinTech industry, outdistancing popular developed markets such as UK and USA with 71% and 46% adoption percentage. Furthermore, the spread of Fintech 3.5 is alleviated by the enhanced use of mobile devices in the society through the reliance of on-the-go functions (Arner, Barberis and Buckley, 2015). This also led to a shift in the mindset of the population to favour convenience more than trust upon physical banking infrastructure (Arner, Barberis and Buckley, 2017).

The innovation in Fintech 3.5 extends beyond the usage and application of technologies, as it incorporates the element of cybersecurity into its service platforms. Among the most popular examples of cybersecurity technologies under Fintech 3.5 includes blockchain, which functions to provide information in a decentralised encrypted platform that flows between specific desired members to uphold data integrity (Ratecka, 2020). This is widely applied in cryptocurrency trading and anti-money laundering efforts. Moreover, this era has also

introduced various breakthroughs such as device-specific cryptograms, two-factor authentication, and biometric solutions. Therefore, Fintech 3.5 has been a significant milestone for the realisation of cybersecurity efforts, making it necessary for the enhancement of simple security measures such as password setting to sophisticated cyber walls such as ethical hacking.

3.0 Cybercrime Platforms of Financial Fraud

Internet is an enormous infrastructure that provides connections to various networks, to facilitate digital payments, banking transactions, online trading platforms and money transfer services. Web, on the other hand is a service that utilises internet to provide information to users (Beshiri and Susuri, 2019). Due to the large content of information, transactions and storage databases that are integrated and communicated in the web through Internet, cyber criminals utilise this opportunity to commit financial fraud. Web can be segregated into two parts of surface web and deep web, in which both platforms are vulnerable to cyberattacks (Beshiri and Susuri, 2019). Surface web is accessible by the general public using normal search engines, such as Google Chrome and Safari. However, this only holds a tiny portion of the internet, about 0.03% (Kaur and Randhawa, 2020). Conversely, deep web is an invisible web that contains private information of companies and databases. It is restricted from public access through secure networks and cannot be accessed through the normal search engines (Chen, 2011).

Delving further into deep web, there lies dark web which is anonymous and intentionally concealed through sophisticated encryption and decentralised nodes to hide IP addresses of the users (Beshiri and Susuri, 2019). The deep web and dark web constitute 96% of the Internet (Kaur and Randhawa, 2020). Although financial fraud occurs in both platforms of surface web and dark web, the additional features of being less regulated and anonymity makes cybercrime activities to be conducted in a greater extend through dark web. A study conducted on the differences in malicious activities of surface web and dark web revealed that leaked honey webmail accounts through paste sites were accessed in a greater scale in Dark Web as compared to Surface Web (Villalva et al., 2018). The duration of exposure of this leaked information is also longer in Dark Web, as the site is not monitored and regulated as stringent as Surface Web. Special types of browsers are used to access Dark Web, comprising The Onion Router (TOR) and Invisible Internet Project (I2P) (Kaur and Randhawa, 2020). TOR transmits multiple relays of nodes through its virtual tunnels when accessing through its browser to conceal the IP address of the user, to remain anonymous. I2P functions as a network within the internet that captures traffic within its network to prevent relays to be transmitted outside its network to ensure privacy and to remain unnoticed. Cybercrimes that are conducted through Surface web and Dark web comprises, credit card frauds, bitcoin scams, money laundering, ransomware and ATM malware (Kaur and Randhawa, 2020).

4.0 Tools and Applications of Cybersecurity

Financial fraud can be interpreted as an illegal act performed by perpetrators with an aim of financial gain. With the advancement in technology, financial fraud is vastly conducted in cyberspace, entailing credit card fraud, forgery, identity theft, money laundering and phishing social engineering. Prevention and detection of fraud conducted in cyberspace demands the use of technology and intelligence tool to encrypt files and obtrude complex systems in virtual environment.

4.1 Neural Networks

Neural networks can be regarded as systems that has a collection of nodes that model the neurons in a biological brain (Fu et al., 2016). It is also known as multilayer perceptron, having the ability to conduct supervised learning on the predictive and non-predictive patterns. Neural network technology was designed with an aim to establish a virtual system, with the combination of artificial intelligence to mimic the human brain (Raudha and Saeedi, 2019). It is a significant tool that can be utilised by banking systems, which can be applied to detect anomalies, new patterns, unusual behaviour and fraud trends in the system in real time to interact with other systems for intrusion alert. Being adaptive to the new patterns and learning current fraud techniques, neural networks keep the system improving progressively, to identify suspicious interference into the banking systems and organisation databases (Park, 2005). Neural networks are also capable of extracting rules and making cognitive predictions on future frauds based on the past trends of fraud (Ogwueleka, 2011). Hence, the application of neural network will generate efficient and faster detection of financial fraud. However, this tool is associated with a setback of being able to produce an accurate result for large transaction dataset only (Zareapoor, Seeja and Alam, 2012).

4.2 Deep Learning

Deep learning incorporates the system of neural network in its structure, but undergoes a greater level of processing, before releasing the output (Choi and Lee, 2018). The vast number of hidden layers that is embedded into deep learning, allows it to extract huge amount of complex data for self-learning. The algorithms in deep learning allows image recognition, bioinformatics, and speech recognition to be conducted effectively, with self-learning mechanism of feature engineering to detect updated malware, virus, scam or any network attacks (Mahdavifar and Ghorbani, 2019). This means that if a company is under an attack of a zero-day malware, this deep learning system will automatically be able to engineer its features to prevent intrusion. This is an upgrade of the machine learning model, in which the algorithms of deep learning are able to capture and predict outcomes accurately, as opposed to the machine learning model that requires human intervention to make adjustments in its prediction. Hence, this deep learning-based cybersecurity is prominent in malware detection and analysis, anomaly detection, phishing detection, spam detection and website defacement detection (Mahdavifar and Ghorbani, 2019).

4.3 BOAT Data Analysis

Bootstrapped Optimistic Algorithm for Tree construction (BOAT) is a model that constitutes a genetic algorithm calculation and analyses customer behaviour (Choi and Lee, 2018). This model is most useful in detecting anomalies in the banking system, especially in credit card fraud. The application of this model can be segregated into two stages. In the first stage, this system is able to detect unusual patterns by comparing it with historical transactions. Extending into the second stage, the suspected anomalies will be compared against the fraud history database for any false alarms (Choi and Lee, 2018). It would then determine if the unusual patterns are of fraudulent transactions or due to legitimate reasons. Hence, this model can be regarded to be adaptive to the discrepancies in patterns and trends of customers as it has a high-level of clustering capacity and incremental update ability. The advantage of utilising this algorithm is that it is able to detect fraud under a maximum coverage, in a quick manner with less cost (Makki, 2019).

4.4 Genetic Algorithm

Genetic Algorithm is a tool that is of evolutionary algorithms, to improve and enhance the search of solutions for fraud through a combination of techniques and applications (Vats, Dubey and Pandey, 2013). It has the ability to scrutinize on advanced problem-solving technique as time progresses. With an aim to eliminate fraud, it is prominent in the development of a secure electronic payment system, in which it helps to detect and prevent fraudulent transactions (Patel and Singh 2013). Besides being a dynamic method in eliminating fraudulent transactions, genetic algorithm is also efficient in reducing the number of false alerts. It also portrays a great level of compatibility and performance, when being applied jointly with other tools. Genetic algorithm has been utilised collectively with support vector machine for bankruptcy prediction, have collaborated with neural network algorithm for accurate credit card fraud detection and have jointly been used with artificial immune system to minimise the rate of false alarm in fraud detection (Zareapoor, Seeja and Alam, 2012). Hence, being a viable tool for cybersecurity, companies could opt for this inexpensive method to have an efficient fraud detecting system (Zareapoor, Seeja and Alam, 2012).

4.5 Tools used by Special Government Agencies

4.5.1 Network Investigative Technique

This tool, which was previously known as Computer and Internet Protocol Address Verifier (CIPAV), is used by the Federal Bureau of Investigation (FBI) to detect and track the perpetrators of cybercrime who are conducting illegal activities in anonymity (Kaur and Randhawa, 2020). This tool is used by the FBI under special permission, to investigate the cases of cyberterrorism. It is mainly used to locate suspects who tries to access the system by illegal software through anonymous servers such as TOR (Rubasundram, 2019). The software helps to segregate the usual internet traffic from the anonymous traffic to focus their search on the suspected network. Consisting of several components of generator, exploit, payload and a logging server, this method will enable the FBI to have a record of the fraudster's computer in their system. Once the user's laptop is accessed, the FBI will be able to collect information of the user such as the IP address, list of programs running, coding language and registered computer name to take further legal actions on the fraud perpetrators (Rubasundram, 2019).

4.5.2 Memex

This tool was established by Defense Advanced Research Projects Agency (DARPA) of the United States, with an aim to enhance information discovery and data mining techniques to separate and segregate needed information from the large amount of database (Kaur and Randhawa, 2020; DARPA, 2018). The Memex program was launched to allow military and government agencies to uncover anomalies in the dark net, to identify transactions of illegal activities that includes, money laundering, illegal weapon market and human trafficking. The structure of Memex was formulated with eight open-sources, browser-based search, analysis and data visualisation programs and back-end server software, to enable the program to conduct high-level complicated evaluation of data (Hammonds, 2015). This is helps to improve the efficiency of investigators in identifying the tactics used by the cybercriminals in committing fraud.

5.0 The Regulatory Environment of Cybersecurity

The alarming concern of security in cyberspace is demanding the role of strong and efficient regulations to govern the aspect of Fintech in various levels. In the early stages, the Fintech industry was not perceived by regulators to be financial in nature, but to be more towards the area of technology, hence, principles established were not focused on financial regulations (Knewtson and Rosenbaum, 2020). However, regulatory sandboxes were then implemented to enable financial technology to be tested under a set of principles and supervision with lower cost of innovation and entry barriers (UNSGSA, 2020). Being officially launched in 2015, U.K. pioneered the application of regulatory sandboxes, followed by more than 20 jurisdictions practicing this concept, including Singapore, Hong Kong, Australia, India, Canada, Malaysia, and Japan (Goo and Heo, 2020). Numerous regulatory boards were also established to administer the activities and areas of concern for Fintech such as Financial Industry Regulatory Authority, The International Token Standardization Association and The Global Digital Finance Group (Knewtson and Rosenbaum, 2020). Cyberthreat Defense Report 2020 reveals the list of countries that were severely affected by ransomware in the past 12 months. This list includes China, at the top spot with (76.0%), Mexico (72.7%), USA (69.5%), South Africa (54.2%) and many more (Cyber Egde Group, 2020).

These countries exhibit coherence in terms of loopholes in their regulations and weak cyber laws. Tambo and Adama (2017) have reported that only 11 out of 54 countries in Africa have implemented cybersecurity laws and regulations. The cyber security awareness in Africa is still weak, as legal institutions are still not enforcing stringent cyber laws to regulate the occurrence of fraud. According to Yingying and Zhengqing (2016), 10 countries in Africa have chosen to develop national cyber security strategies, with specialised cybercrime laws adopted by 5 countries and data protection laws developed by 7 countries. South Africa have also passed Electronic Communications and Transactions Act in 2002, with an aim to administer transactions that are conducted via electronic means. Although South Africa has developed a basic structure of governance for cybersecurity, it cannot be assured that the regulations established are sufficient to prevent complex intrusion of systems. One of the challenges of cybersecurity governance faced by Africa includes limitation in the technical capacity (Yingying and Zhengqing, 2016).

Besides, no specific regulation is also dedicated in governing the laws pertaining cybersecurity in Mexico. Although Mexican Fintech Law was introduced in March 2018, to govern areas around cryptocurrencies and crowdfunding institutions, no rigid laws were established on the anonymity concerns in the cyberspace (Lexology, 2020). In the regulatory environment of Turkey, it can be observed that there are various regulations that governs its Fintech aspect. The regulations include “Banking Law no. 5411, Law no. 6493 for Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions and Bank and Credit Cards Law no. 5464” (Degerli, 2019). These regulations are predominant in regulating the banking and payment services of Turkey. The regulations for anti-money laundering and counter-terrorism financing have also been passed in Turkey. Although there are numerous legislations that covers the different scope of Fintech, the challenge in this situation is the matter of compliance. The need for companies to comply to a large number of regulations in each aspect of their business process such as Payment Systems Law and Credit Card Laws hinders the efficiency of their service (Degerli, 2019).

Therefore, a comprehensive set of corroborating regulations could assist better for the Fintech industry in Turkey. Moreover, the issue of violation of privacy also arises as law enforcement allows special government agencies to use software and tools to conduct online surveillance and track malicious activities (Rubasundram, 2019). When the authorities hack into TOR networks with a warrant from the legal departments, it could be a situation in which the accounts of the other innocent users may have been hacked to track the activities of users. Therefore, legal authorities have to strengthen regulations, with a reflection on the balance between the issue of privacy and security to ensure all corporations and agencies are abiding by the law enforcement for efficient transactions in cyberspace.

6.0 Challenges of Cybersecurity Solutions

The impeccable limelight on technology commands a greater desire for cybersecurity. It is of an undeniable importance in ensuring the safety of transactions and protection of governmental, industry and personal information. However, the execution of proper cybersecurity measures comes with some challenges, in which individuals, organisations and government agencies must be conscious about.

6.1 Cost

The effectiveness of the cybersecurity solutions for companies are also associated with the price factor. A complex system that is equipped with comprehensive and complicated data mining and financial fraud detection ability would be astronomical, in terms of the cost. This threat would be greater for smaller organisations, as they will face the same risk of financial fraud as large corporations, but with a smaller scale of resources (Skeleton, 2017). Additional costs would also be needed to be borne for regular system updates and compliance costs. As small companies go through the process of expansion to venture into a wider geographical scope, the different regulatory structures in various regions could drive the costs even further. The cost of hiring skilful IT personnel to maintain and monitor the cybersecurity programs would also be an extra burden for small companies. However, there are also situations in which companies have overspent on security measures, with lack of supervision on its effectiveness and full capacity utilisation, gaining the minimal amount of benefits with inflated costs (Skeleton, 2017).

6.2 Regulatory Challenges

The establishment of prudent Fintech regulations are crucial in ensuring that cybersecurity programs are conducted in a seamless manner. However, it must be apprehended that standard regulations pertaining Fintech and comprehensive global cyberlaws are deficient, due to complications in regulatory framework and the novelty of Fintech technology (Skeleton, 2017). As the tools of artificial intelligence evolve with extended usage around the world, it needs to comply with the laws and regulations stipulated in different areas (Ng and Kwok, 2017). The regulatory uncertainties surrounding the legal aspect of usability of cybersecurity tools and the extent of use, poses risks, as it may be viewed as loopholes by cybercriminals. Besides, the variability of regulatory requirements may also create greater complications for small organisations. There are also less strict regulations concerning the accessibility of anonymous websites, to ensure that the activities of cybercriminals can be traced down easier, with less concerns about privacy. The issue of ethical dilemma can also be associated as part of the

regulatory challenges for cybersecurity. For example, in the investigation of Playpen website on the dark web, FBI utilised Network Investigative Technique, with the permission of federal court to get access into the computer server of Playpen, and continued to operate the site using their own networks for two weeks, in an effort to discover 1300 IP addresses of visitors on the website (Rubasundram, 2019). In this situation, although the regulators have provided approval to conduct their hacking investigative techniques to prosecute cybercriminals, the ethical element in this scenario is challenged as the dilemma of whether the FBI were ethically right when operating the child pornography website arises, although it was deemed for a good cause. Another question of ethics that can be raised includes, the surety of the investigators of not misusing the website after getting access to it.

6.3 Lack of Awareness

Organisations and government, especially in less developed countries may underestimate the need for strong cybersecurity measures (Ng and Kwok, 2017). Such situations could make them more vulnerable to cyberattacks, as their level of preparedness for system intrusions would be low. In some cases, government would have developed necessary policies for cybersecurity, but the organisations could be less conscious about its importance. Companies may not have established a department of cyber defence in their business structure, allowing third party vendors to gain access into their system for malicious intent. For example, Carbanak attacks were conducted by installing malware into the bank's system through spear phishing emails to defraud a hefty amount reaching $1 billion USD (Skeleton, 2017). Therefore, organisations have to dedicate greater attention to the need of having proper internal controls and hiring personnel with IT knowledge to prevent and detect these financial frauds.

6.4 System Enhancement

Improvements on cybersecurity algorithms and mechanisms are crucial to be updated in a routine manner. As cybercriminals become more creative and innovative in introducing malwares and anonymous routes in intruding systems, the IT experts would need to exert a greater level of dedication to discover methods to prevent and detect these attacks (Sujitparapitaya, Shirani and Roldan, 2012). This would demand more time, cost and energy from the IT experts. There is no boundary for the development in technology, hence IT experts should not be contented with the level of existing security solutions. For example, the development of antivirus deemed to be a powerful tool in preventing, detecting, and removing malware from computer systems a few decades ago. However, in this bleeding age of technology, the question of adequacy of the antivirus software arises, as complex and updated version of viruses and tactics are developed to hack into systems. Therefore, the burden of IT researchers to update and improve cybersecurity systems poses threats to individuals, organisations and governments.

7.0 Conclusion

With the evolution in technology, abundance of tasks are conducted virtually, from mobile banking, crowdfunding, insurtech to robo-advising, affecting the individuals, organisations and governments at all levels. However, there are also setbacks that comes along with this advancement if technology is used by fraudsters with malicious intent. This paper has reviewed the aspect of cybersecurity in protecting and providing a safer virtual environment for

transactions and negotiations to occur in a more secure manner. The platforms of which cybercriminals often utilise to intrude into organisation's systems have been explored. Dark web has a greater extend of usage and are relied more by fraudsters, as opposed to surface web, due to the concept of anonymity and less regulations. With regards to that, cybersecurity tools and algorithms such as neural networks, deep learning, BOAT data analysis, genetic algorithm and special tools used by government agencies were also discussed and associated with the function of preventing and detecting financial fraud. For the purpose of understanding the usage of technology, which includes cybersecurity innovations, regulatory sandboxes were adopted to benefit both Fintech companies and regulators in facilitating the innovations, to determine if the solutions provide positive impacts to the organisations and to the market.

However, considering that many countries are still yet to adopt this regulation, it is tough for these companies to be on a par with other countries that have established regulatory sandboxes, in terms of the growth and innovation of Fintech technologies, including cybersecurity solutions. Lack of stringent and comprehensive set of uniform cyberlaws also pose hindrance to the efficiency of businesses and organisations. The prominent element of ethics also becomes a huge question in the application of cybersecurity tools by special government agencies, such as the FBI in accordance with the stipulation of law. Cybersecurity solutions also pose challenges, in terms of the matter of cost, legal frameworks and laws, inadequate awareness, and the burden of being vigilant to continuously update systems.

Therefore, it takes more than the role of an individual or an organisation to implement successful cybersecurity measures to ensure a safe networking environment in cyberspace. A collaborative effort from organisations, government and cross-country participation would further enhance the efficiency and effectiveness of the cybersecurity solutions. Future research could exert prominence in exploring the hurdles faced by organisations during the implementation process of cybersecurity solutions and the key performance indicators that can be relied by organisations in ensuring that the ultimate goal of implementation is attained systematically.

8.0 References

Arner, D.W., Barberis, J. and Buckley, R.P. (2015) The evolution of Fintech: A new post-crisis paradigm. *SSRN Electronic Journal.* [Online]. 47. p.1271. Available from: http://dx.doi.org/10.2139/ssrn.2676553. [Accessed: 10 March 2021].

Arner, D.W., Barberis, J. and Buckley, R.P. (2017) FinTech and RegTech in a Nutshell, and the Future in a Sandbox. *Research Foundation Briefs.* [Online]. 3 (4). pp. 1-20. Available from: https://www.cfainstitute.org/-/media/documents/article/rf-brief/rfbr-v3-n4-1.ashx. [Accessed: 12 March 2021].

Beshiri, A.S. and Susuri, A. (2019) Dark web and its impact in online anonymity and privacy: A critical analysis and review. *Journal of Computer and Communications.* [Online]. 7 (03). p.30. Available from: http://dx.doi.org/10.4236/jcc.2019.73004. [Accessed: 7 March 2021].

Chen, H. (2011) *Dark web: Exploring and data mining the dark side of the web*. Vol. 30. London: Springer Science & Business Media. [Accessed: 7 March 2021].

Choi, D. and Lee, K. (2018) An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation. *Security and Communication Networks* [Onine]. 2018 Available from: http://dx.doi.org/10.1155/2018/5483472. [Accessed: 10 March 2021].

Cyber Edge Group (2020) *2020 Cyberthreat Defense Report*. [Online]. Available from: https://cyber-edge.com/wp-content/uploads/2020/03/CyberEdge-2020-CDR-Report-v1.0.pdf. [Accessed: 8 March 2021].

DARPA (2018) *Defense Advanced Research Projects Agency.* [Online]. Available from: https://www.darpa.mil/attachments/DARAPA60_publication-no-ads.pdf. [Accessed: 8 March 2021].

Das, S.R. (2019) The future of fintech. *Financial Management* [Online]. 48 (4). pp.981-1007. Available from: http://dx.doi.org/10.1111/fima.12297. [Accessed: 10 March 2021].

Degerli, K. (2019) Regulatory Challenges and Solutions for Fintech in Turkey. *Procedia Computer Science* [Online]. 158. pp. 929–937. Available from: http://dx.doi.org/10.1016/j.procs.2019.09.133. [Accessed: 9 March 2021].

Ernst & Young (2019) *Global FinTech Adoption Index 2019.* [Online]. Available from: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-global-fintech-adoption-index.pdf. [Accessed: 12 March 2021].

Fu, K., Cheng, D., Tu, Y. and Zhang, L. (2016) Credit card fraud detection using convolutional neural networks. In *International Conference on Neural Information Processing* [Online]. 9949. pp. 483-490. Available from: https://doi.org/10.1007/978-3-319-46675-0_53. [Accessed: 10 March 2021].

Goo, J. J. and Heo, J. Y. (2020) The impact of the regulatory sandbox on the fintech industry, with a discussion on the relation between regulatory sandboxes and open innovation. *Journal of Open Innovation: Technology, Market, and Complexity* [Online]. 6 (2). Available from: http://dx.doi.org/10.3390/JOITMC6020043. [Accessed: 7 March 2021].

Hammonds, J. (2015) An Inquiry into Privacy Concerns: Memex, the Deep Web, and Sex Trafficking. [Online]. Available from: http://www.infosecwriters.com/Papers/JHammonds_Privacy.pdf. [Accessed: 10 March 2021].

Kaur, S. and Randhawa, S. (2020) Dark Web: A Web of Crimes. *Wireless Personal Communications*. [Online]. 112 (4). pp. 2131–2158. Available from: http://dx.doi.org/10.1007/s11277-020-07143-2. [Accessed: 7 March 2021].

Knewtson, H. S. and Rosenbaum, Z. A. (2020) Toward understanding FinTech and its industry. *Managerial Finance*. [Online]. Available from: http://dx.doi.org/10.1108/MF-01-2020-0024. [Accessed: 7 March 2021].

Lexology (2020) Data Security and Cybercrime in Mexico. [Online]. Available from: https://www.lexology.com/library/detail.aspx?g=4fcfea5a-0d5f-4702-9925-917c98db9877#:~:text=There%20is%20no%20dedicated%20law,and%20cybersecurity%20law%20in%20Mexico. [Accessed: 8 March 2021].

Mahdavifar, S. and Ghorbani, A. A. (2019) Application of deep learning to cybersecurity: A survey. *Neurocomputing*. [Online]. 347. pp. 149–176. Available from: http://dx.doi.org/10.1016/j.neucom.2019.02.056. [Accessed: 12 March 2021].

Makki, S. (2019) *An Efficient Classification Model for Analyzing Skewed Data to Detect Frauds in the Financial Sector*. A Thesis Submitted for Degree of Doctor of Philosophy. Université de Lyon; Université libanaise. [Online]. Available from: https://tel.archives-ouvertes.fr/tel-02457134/. [Accessed: 10 March 2021].

Nasir, F. and Saeedi, M. (2019) "RegTech" as a Solution for Compliance Challenge: A Review Article. *Journal of Advanced Research in Dynamical and Control Systems*. [Online]. 11 (11 Special Issue) pp. 912–919. Available from: http://dx.doi.org/10.5373/JARDCS/V11SP11/20193115. [Accessed: 6 March 2021].

Ng, A. W. and Kwok, B. K. B. (2017) Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. *Journal of Financial Regulation and Compliance.* [Online]. 25(4). pp. 422–434. Available from: http://dx.doi.org/10.1108/JFRC-01-2017-0013. [Accessed: 6 March 2021].

Ogwueleka, F.N. (2011) Data mining application in credit card fraud detection system. *Journal of Engineering Science and Technology* [Online]. 6 (3). pp.311-322. Available from: http://jestec.taylors.edu.my/vol%206%20issue%203%20junel%2011/vol_6(3)_311%20-%20322_ogwueleka.pdf. [Accessed: 7 March 2021].

Park, L.J. (2005) Learning of neural networks for fraud detection based on a partial area under curve. In *International Symposium on Neural Networks* [Online]. pp. 922-927. Available from: https://doi.org/10.1007/11427445_148. [Accessed: 6 March 2021].

Patel, R.D. and Singh, D.K. (2013) Credit card fraud detection & prevention of fraud using genetic algorithm. *International Journal of Soft Computing and Engineering*. [Online]. 2 (6). pp.292-294. [Accessed: 9 March 2021].

Ratecka, P. (2020) FinTech—definition, taxonomy and historical approach. *The Małopolska School of Economics in Tarnów Research Papers Collection*. [Online]. 1 (45). pp.53-67. Available from: http://dx.doi.org/10.25944/znmwse.2020.01.5367. [Accessed: 10 March 2021].

Raudha, F. and Saeedi, M. (2019) Artificial intelligence and machine learning as a tool in preventing and detecting financial fraud: A systematic literature review. *Journal of Advanced Research in Dynamical and Control Systems.* [Online]. 11(11 Special Issue). pp. 904–911. Available from: http://dx.doi.org/10.5373/JARDCS/V11SP11/20193114. [Accessed: 8 March 2021].

Rubasundram, G. A. (2019) The dark web and digital currencies: A potent money laundering and terrorism opportunity. *International Journal of Recent Technology and Engineering*. [Online]. 7 (5), pp. 476–482. Available from: https://www.semanticscholar.org/paper/The-Dark-Web-and-Digital-Currencies%3A-A-Potent-Money-Rubasundram/b8260c993cb6bd666517b6ab03eea5f96e89e604. [Accessed: 9 March 2021].

Setiawan, K. and Maulisa, N. (2020) The Evolution of Fintech: A Regulatory Approach Perspective. *Advances in Economics, Business and Management Research.* [Online].

130. pp. 218-225. Available from: https://dx.doi.org/10.2991/aebmr.k.200321.029. [Accessed 12 March 2021].

Skelton, A. (2017) Analyzing Cyber Threats Affecting the Financial Industry. [Online]. Available from: https://www.semanticscholar.org/paper/Analyzing-Cyber-Threats-Affecting-the-Financial-Skelton/3a5a837a1f3703043fd71e278f8c87068daa4b9d. [Accessed: 9 March 2021].

Sujitparapitaya, S., Shirani, A. and Roldan, M. (2012) FinTech, RegTech and the importance of cybersecurity. *Issues in Information Systems*. [Online]. 13 (2). pp. 112–122. Available from: http://dx.doi.org/10.1037/a0031073. [Accessed: 7 March 2021].

Tambo, E. and Adama, K. (2017) Promoting cybersecurity awareness and resilience approaches, capabilities and actions plans against cybercrimes and frauds in Africa. *International Journal of Cyber-Security and Digital Forensics*. [Online]. 6 (3). pp.126-138. Available from: http://dx.doi.org/10.17781/P002278. [Accessed: 6 March 2021].

UNSGSA (2020) *Briefing on Regulatory Sandboxes.* [Online]. Available from: https://www.unsgsa.org/files/1915/3141/8033/Sandbox.pdf. [Accessed: 10 August 2020].

Vats, S., Dubey, S.K. and Pandey, N.K. (2013) Genetic algorithms for credit card fraud detection. In *International Conference on Education and Educational Technologies*. [Online]. Available from: https://www.researchgate.net/publication/339915930_Genetic_algorithms_for_credit_card_fraud_detection#:~:text=A%20genetic%20algorithm%20is%20an,detection%20system%20to%20be%20tested. [Accessed: 10 March 2021].

Villalva, D.A.B., Onaolapo, J., Stringhini, G. and Musolesi, M. (2018) Under and over the surface: a comparison of the use of leaked account credentials in the Dark and Surface Web. *Crime Science* [Online]. 7 (1). pp.1-11. Available from: http://dx.doi.org/10.1186/s40163-018-0092-6. [Accessed: 11 March 2021].

Yingying, X. and Zhengqing, Y. (2016) A primary exploration on cyber security governance in Africa. *West Asia and Africa*. [Online]. 2016 (3). pp.121-137. Available from: http://en.iwep.org.cn/papers/papers_papers/201707/W020170727532114330688.pdf. [Accessed: 6 March 2021].

Zareapoor, M., Seeja, K.R. and Alam, M.A. (2012) Analysis on credit card fraud detection techniques: based on certain design criteria. *International journal of computer applications*. [Online]. 52 (3). Available from: https://pdfs.semanticscholar.org/8c48/05a11949ae979c126749ebb88d56b3b41336.pdf. [Accessed: 8 March 2021].