International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Keyboard Acoustic Side Channel Attacks on Android Phones in the AI Era of Digital Banking: An Elementary Review

Mamta B Savadatti[1], Nikita J. Kulkarni[2], Geetanjali Devendra Bansod[3], Paramita Sarkar[4], Praveen Kumar[5], Kumar Sargam[6] , Payal Gulati[7] and Ajay Sudhir Bale[*8]

Submitted: 04/09/2023 **Revised :** 22/10/2023 **Accepted :** 07/11/2023

Abstract: The banking and finance industry has seen immense transformation as a result of the growth of financial technology (FinTech) in areas including wireless Internet, big data, cloud computing, internet search engines, and blockchains, requiring conventional banks to modernize. The so-called "AI effect" describes how actions formerly deemed to need "intelligence" are often dropped with the perspective of AI as machines get greater abilities. It's established that keyboard acoustic side channel attacks may use the audible emission from keystrokes to roughly guess the passwords/PINs that were entered. By using numerous methods and vectors of attack, including triangulation, keypad geometry, and extraction of features and categorization, experts have kept trying to increase the effectiveness, but a lot of effort has been missing in creating a functional defence mechanism against this type of attacks, even though research is continuously being done to better improve acoustic side channel attacks. The article examines the safety risks and holes in online banking, it also offers a thorough analysis of side-channel attacks (SCA) unique to digital banking in the era of AI, which hasn't been done before. Current research issues and possible future avenues are also covered in the paper.

Keywords: *Side-channel attacks; security threats; cryptography; digital banking; online banking; cyber-security*

1. Introduction

Artificial Intelligence (AI) has undergone many stages of confidence, disappointment, and financing losses ever since it was first studied academically in 1956, before experiencing innovative ideas, success, and increased funding. Several other approaches to study of artificial intelligence have been studied investigated and discarded, include brain replication, simulating intellectual troubleshooting, logical thinking, massive collections of data, and imitating animal behaviour. Machine learning with a strong analytical and numerical focus characterized the field in the early years of the 21st century. This method was extremely successful in helping to solve a wide range of challenging problems in both industry and academia.

AI is intelligence exhibited by machines—perceiving, synthesising, and determining information—as compared to intelligence shown in people or other living things. "Intelligence" refers to the capacity to acquire knowledge, logic, generalise, and derive meaning. Automatic speech recognition, computer vision, translations across various languages, and other data translations are examples of jobs where this is done. Sophisticated web searches (e.g., Google Search), recommendations systems (which is utilised by Amazon, YouTube, and Netflix), on the contrary understanding human speech, autonomous vehicles creative or creative tools, autonomous decision-making, and battling at the most advanced levels in strategic board games like a chess and Go instances that demonstrate uses for AI. [1]

The impact of AI happens whenever tasks that were formerly thought required "intelligence" are no longer seen to require it as robots become more capable. For instance, although being a widespread technology, recognition of optical characters is often left out of what is referred to as AI.

A SCA uses tracking or indirect implications of the system

[1] *Dept. of ECE, New Horizon College of Engineering, Bengaluru, India; mamta.savadatti@gmail.com*
[2] *Associate Professor, K J College of Engineering and Management Research, Pune, Computer Engineering Department; nikitakulkarni.kjcoemr@kjei.edu.in*
[3] *Assistant Professor, KJ College of Engineering management and research, Pune, Computer Engineering Department; geetanjalibansod.kjcoemr@kjei.edu.in*
[4] *Assistant Professor, Department of C.S.E, JIS UNIVERSITY, ORCID: 0000-0002-2330-8484; paramita.sarkar@jisuniversity.ac.in*
[5] *Professor & Head, Department of Mathematics and Computer Science, J V Jain College Saharanpur UP-247001(Bharat); peerudma77@gmail.com*
[6] *Department of Theatre & Music, Lovely Professional University, Phagwara India; kukusa221@gmail.com*
[7] *Assistant Professor, Department of Computer Engineering, J.C. Bose UST, YMCA, Haryana; gulatipayal@yahoo.co.in*
[8] *Dept. of ECE, New Horizon College of Engineering, Bengaluru, India; ajaysudhirbale@gmail.com*
** Corresponding Author Email: ajaysudhirbale@gmail.com*

or its infrastructure to gather data or change the software that controls the system as a whole. In brief, a SCA exploits evidence that was unintentionally leaked by a computer to break encryption [2]. These attacks are posed by components with inbuilt cryptography mechanisms. Many strong computational crypto processes were effectively cracked by side-channel research methods. The aim of this research is to provide an overview of the various side channels attacks and defences in systems for online banking.

Typically, data secrecy in a computer network is provided using data encryption, which encrypts plain text into unreadable (cypher) text. Cryptography is carried out practically in computers. Energy utilisation, acoustic emission levels, timing, and temperature fingerprints all give significant data that may be used to decrypt the encryption standard and keys. Side-channel attacks (SCAs) involve the collection of data via the functioning of physical components [3].

Internet connectivity has helped first generation banking transition into second generation banking, and owing to the rapidly developing usage of smartphones, third generation banking has emerged when it comes to categorizing bank advancements throughout the previous several decades. Currently, 3rd generation banking is evolving towards 4th generation banking, although not because of unique advances, but rather because it represents the spread and maturation of new inventions like ML and virtual reality, as shown in Figure 1, as well as the increasing use of these technologies.

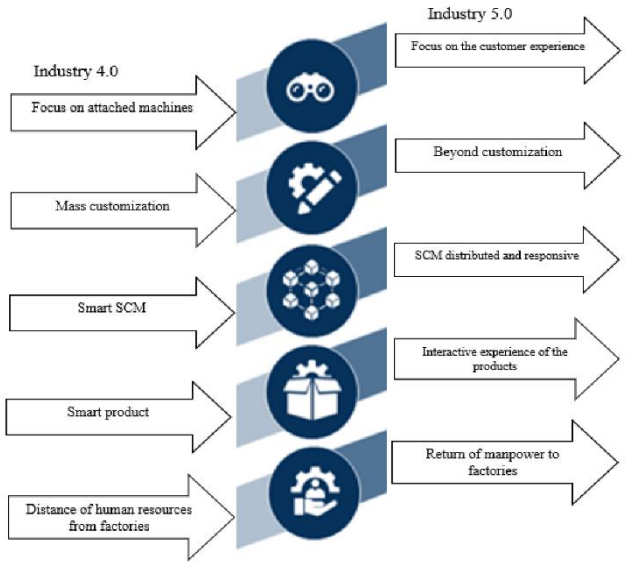

Fig. 1. Digital Banking transformation [4]

Speech recognition systems, which are influential for improving the banking industry and addressing contemporary issues of financial institutions that are restructuring the way they operate towards internet-based banking in order to accomplish a rapid rise in the financial sector[5]. Given the significance of financial systems, Meher et al.[6] describe online banking to be the "transformation of traditional bank whereby individuals had to be physically present at the bank branch for transactions involving money.

2. Related Work

Scientists learned that equipment might unintentionally leak material by electromagnetic, visual, or acoustic noise in the beginning of the 1960s, such as in [7-9]. This kind of effort, which involves learning information via unintentional release assessment and stopping releases from escaping, is referred to as TEMPEST in the security and defense industries [10]. There are other methods as well, such recovering printed documents from printer noise or reassembling transmitted information from communication devices using LED status lamps [11].

Numerous research attempted to track footage using magnetic and visual emissions as the technology for displays evolved [12-14]. A side-channel method to obtain a PIN from the display of a cell phone is provided by the researchers of [15]. The attack was built by employing a pair of microphones or loudspeakers installed in a cell device to listen to the digit taps when the PIN is entered. The location of each and every sound source was determined by the authors using the Time Difference of Arrival (TDOA) method, which was subsequently aligned with the Keypad design to determine the character/digit with a greater than 50% reliability. The work's flaw was that the authors attempted to isolate a single letter or number rather than the whole PIN each time. PIN input sounds (fast taps) may all sound the same, leading to inaccurate digit placement. In their work published in [16], the authors provide the mathematical framework that they utilized to create an attack that recovered characters and digits from a victim's mobile phone screen.

The attack makes advantage of prior information, such as the victim's cellphone's placement in relation to the attacker's whereabouts and field of study. The authors claim that in order to accurately determine the character or digit tap information, the victim and the opponent must be closer than 60 cm. However, the authors of [17] provide an acoustic side-channel method that recovers the lock patterns by making advantage of the microphone included into an Android smartphone. The authors use a mobile application to collect the radiation of the lock structure, perform a noise reduction filter, signals division, and relative motion measurements, and finally analyze the pattern of the fingers.

The author advises utilizing changing patterns instead of linear ones to increase security and claims a 72% success rate in recovering screen locking passwords. These

successive attacks on the display allow us to draw the conclusion that the technology of the target devices has a substantial impact on reconstructing information from emissions. Keypads work the same way. Keypads' physical construction may produce a range of pollutants, include vibrations and noises. By gaining access to hardware, side-channel analysis tries to reconstruct plaintext, passwords, or other data. In general, the SCA is not hostile. It aims to gather data via the device's timing [18] and power utilization [19] rather than making direct attacks on the information. It has been shown that acoustic SCA are possible [20]. The aforementioned instances lead us to the conclusion that we must take side-channel information leakage into consideration when creating safety features for digital financial services.

3. Android Ecosystem

A detailed list of the Android-powered devices is shown in Figure 2. The graphic makes it easier for the reader to understand the enormous diversity of Android-powered devices utilized by all significant industrial companies.
Even if academics are working to raise mobile manufacturers' awareness of inventiveness, newness, and safety via user-friendly regulations, authentication systems, and safety standards [21]. However, there are still a number of Android issues that need to be fixed. As the platform develops, more recent risks and vulnerabilities are continuously discovered and published, making it challenging for researchers to fix the problems as soon as they are made public. Additionally, a large number of the publicly publicized vulnerabilities are not easily patchable and need extensive study. As a result, these vulnerabilities often need to be fixed for lengthy periods of time, leaving Android users vulnerable to attackers. Since its debut, Android has had almost 4000 vulnerabilities found [22-23]. The 3Tier security approach, which is used to safeguard Android smartphones at the border, contains [24]
(1) Security precautions delivered by SE-Linux
(2) security precautions offered by Google, and
(3) security precautions provided by the original equipment manufacturer (OEM).

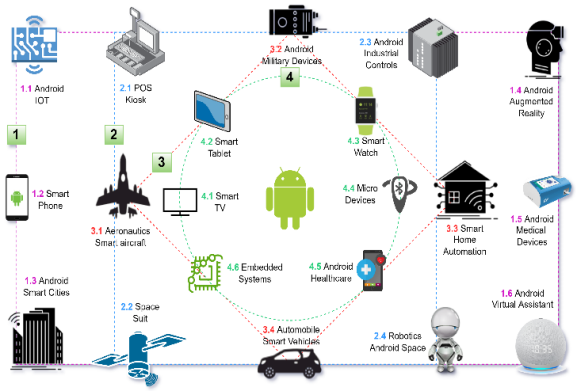

Fig. 2. Detailed overview of Android devices [24]

4. SCA

Acoustic side-channel attacks in digital banking are a kind of attack in which attackers use audio emissions from computer systems to gather information about the devices' internal functions. While not as widespread as some other side-channel attacks, it is a possible attack vector that security researchers and practitioners should be aware of. Here's how acoustic side-channel attacks could impact online banking:

Acoustic side-channel attacks may be used to deduce keystroke performed by a user on a physical keyboard. Attackers may be able to derive personal data, including credentials, PINs, or other authentication credentials by analysing the noises made when keys are pushed. Acoustic emissions during cryptographic processes may possibly reveal information about the activities being conducted. The exact pattern of sounds released during encryption or decryption procedures as shown in Figure 3, for example, might provide information about the encryption keys or the data being processed [24].

- Authentication Bypass: If a digital banking application employs sound-based authentication techniques (for example, analysing unique sound patterns generated when users interact with their devices), attackers may try to recreate or manipulate these sound patterns in order to obtain unauthorised access to accounts.

- Transaction Analysis: Certain financial transactions or procedures may generate different sound patterns that attackers may analyse. This information might assist them in determining the sort of transaction or the amount involved.

- Physical Device Manipulation: Attackers may utilise acoustic side-channel attacks to get knowledge into physical device manipulation. They may, for example, analyse noises made with the placement or elimination of actual tokens or cards.

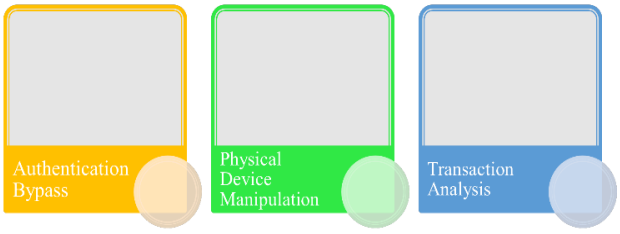

Fig. 3. Acoustic pattern during encryption and decryption in digital banking

4.1 Acoustic Side-Channel Attack Mitigation:

Several efforts as depicted in Figure 4. may be taken to reduce the danger of acoustic side-channel attacks in the context of digital banking:

- Physical Isolation: Designing equipment or systems to decrease sound leakage may assist lessen the possibility of acoustic attacks. Noise or sound masking tactics might make it more difficult for intruders to discern significant audio from unnecessary noises in the background.
- Secure Hardware: Using secure hardware design practises may assist to reduce unintentional audio emissions throughout critical activities.
- Monitoring for unexpected noise patterns and analysing the setting of sound emissions might assist in identifying possible attacks or abnormalities.
- Using multi-factor authentication techniques which go outside sound-based authentication may lessen the effect of acoustic attacks on account security.
- User Education: Informing users about the hazards of acoustic side-channel attacks and advocating safe practises may improve overall security awareness.

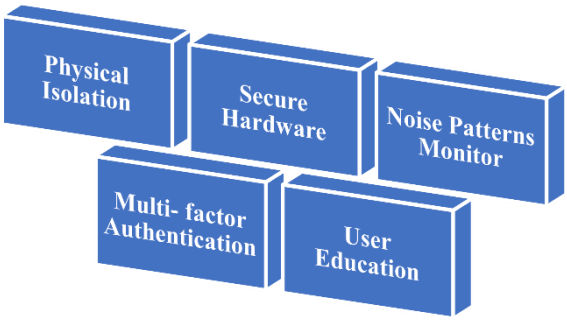

Fig. 4. Different ways to mitigate side channel attacks in digital banking

It's crucial to note that the efficiency of an acoustic side-channel attack is dependent on a number of elements, such the degree of sensitivity of the data targeted, the reliability of the audio capture equipment, and the attackers' competence. Nonetheless, given the ever-changing environment of cybersecurity threats, prospective attack vectors such as acoustic side-channel attacks must be considered when building and defending digital banking systems.

The following security requirements must be completed in order to use online banking services, as well as the creation of a secure connection among the consumer and the financial server [24]. The link that allows data flow among the keyboard and the host is shown in Figure 5.

The transmitted data is only accessible by designated individuals.

Truthfulness: Protection is taken to prevent an attack through identification, and the information transmitted is not susceptible to forgery by another party.

Mutual authorization requires that those involved in communications verify and verify the other's certification outcomes.

Non-repudiation: To be able to refute actions by third parties, communication-related companies must verify the results of their conversations.

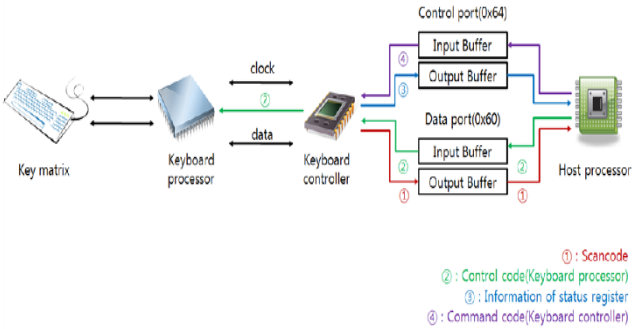

Fig. 5. The transmission of data between the keyboard and the host in digital banking [24].

The total amount of identified SCA vectors is expanding. Among the most typical attacks as depicted in Figure 6 are:

- *Timing attack*: Examines how long it takes an apparatus to run encryption algorithms. Encryption methods optimize encryption operations by varying the length of time it takes to analyze a given key, and TAs take advantage of this variability. As a result, temporal attacks are able to deduce sensitive data by statistical evaluation of time spent processing.

- *Attack using electromagnetic (EM) radiation*: Analyses the electromagnetic radiation that a gadget emits and analyses it. Attacks based on electromagnetic radiation generated by the target encryption equipment are known as EM attacks (EMA). Differential electromagnetic analysis (DEMA) along with straightforward electromagnetic analysis (SEMA) are the two main categories of EM analysis attacks. The SPA and DPA methods of power analysis attacks are used to quantify EM radiation. When measuring the power consumption of the intended system is not possible, these methods come in handy.

- *Simple power analysis (SPA):* Throughout operation, a cryptographic system's power and electromagnetic (EM) fluctuations are directly seen. Attacks based on monitoring and evaluating the variations in electrical power use brought on by the implementation of an encryption algorithm are known as power analysis attacks (PA). It is common practice to classify power analysis attacks as either simple power analysis (SPA)

or differential power analysis (DPA). Power consumption (the power waveform) analysis is at the heart of the SPA attack method, which is used to deduce sensitive data. If one bit of the private key is 0, the RSA encryption algorithm performs an exponential operation; otherwise, it does an exponential operation followed by a multiplication operation. The DPA attack method takes use of the fact that processing the encryption key and associated data in an encryption system results in variable amounts of power consumption. Both the zero and one power consumption change assumptions of Hamming Distance and the one power consumption change assumption of Hamming Weight underpin the DPA attack method [24a].

- *Acoustic Cryptanalysis Attacks (ACA):* Audio-based SCA, or acoustic cryptanalysis attacks (AC), are another kind of cryptanalysis. In this technique, the discrepancy between RSA secret keys 0 and 1 is exploited to increase power consumption and alter the acoustic aspects of CPU operation when CPU use rises. This technique records CPU noise fluctuations as a waveform and then compares that waveform to the plain text to spot operations like multiplication and addition that pertain to the RSA secret key. The discovered operation data is then utilized to deduce the secret key's underlying structure and get it.

- *Differential power analysis (DPA):* It is the process of collecting and analysing specific statistical data from a variety of processes.

- *Template Attack*: Attack using a "template" device to recover cryptographic keys by using a device that's comparable to examine side-channel material.

- *Fault Analysis Attacks (FA):* These are attacks in which an unforeseen flaw is introduced into the hardware or chip used for encrypting data. Fault analysis attacks evaluate the erroneous data produced by the faulty chip or piece of hardware in order to get access to sensitive company data. Whether it's a little piece of information security hardware or a large piece of equipment like a server at an authentication agency, failures may and do happen. Fault analysis attacks may take one of two forms; the first involves physically removing the chip from its packing, while the second employs the generation of an external electrical spark.

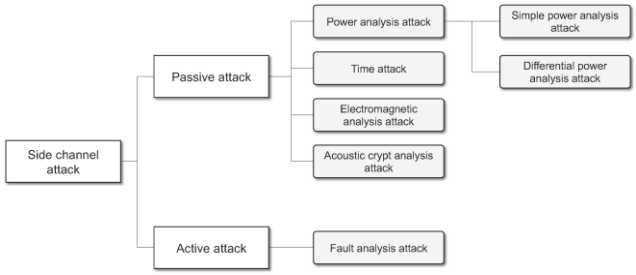

Fig. 6. Vectors in SCA [24a]

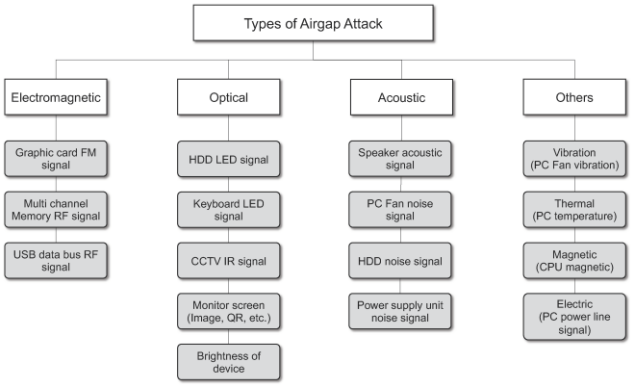

Fig.7. Air-Gap attacks [24a]

As discussed in the earlier section 4 in acoustic side channel mitigation, information must be sent from a private, physically separated network to a public one, which is termed as air-gap attacks. This can be furhter classified and is depicted in Figure 7. As a result, air-gap attackss are restricted in the types of media they may use. Previous research on air-gap attackss has shown that the success of such an attack depends on the configuration of the victim's local computer and its associated hardware. One such technique makes use of the flashing of a hard drive LED to convey information. An alternative involves using the computer's speaker to broadcast information at a frequency outside the range of human hearing. Furthermore, various constraints, including distance and transmission speed, have been shown to exist when actually executing air-gap attackss in the wild.

In light of this, we define air-gap attacks on a fundamental level and explore the conditions under which information may be extracted from a closed network. We also deduce attacks scenarios with detailed steps and environmental conditions for each kind of air-gap attack, and identify media that may be employed in air-gap attacks.

Using the four media kinds of electromagnetic, optical, acoustic, and other (such as magnetic, thermal, power line, and vibration) shown in Figure 7, this study organizes the air-gap attacks methodologies considered. As was previously said, an air-gap attack is a kind of cyberattack in which malware artificially controls data produced by a

computer and its connected peripherals inside a closed network in order to transmit confidential data to a device on an open network. Based on the types of signals that may be created by the computers, peripherals, and smart devices inside the protected network, this article concludes that air-gap attacks can be broken down into many distinct categories. Hard drive LEDs, keyboard LEDs, monitors, and network status LEDs are all examples of lights that may be found within a closed network. Blinking or altering the brightness of the light source is a way for air-gap virus to send information to the outside world after it has gained control of the device. This research demonstrates, in a similar vein, that many sources of noise and electromagnetic waves may be contained inside an isolated system. Devices and components shown in Figure 2 that are compatible with each media.

An air-gap attack is one whereby an attacker obtains the internal sensitive information from a closed system (usually a remote system) and delivers the information to the exterior using optical signals Acoustic, or electromagnetic waves generated by computer hardware and peripheral equipment as the means of transmission. Figure 8 depicts a common air-gap assault setup setting. Behind the closed network is an air-gapped PC infected with malware having air-gap attack features aimed for collecting important data. The air-gap virus captures sensitive information created in the private network, such as passwords, authentication keys, key logs, and internal network architecture, invisibly. The information gathered is encoded as a digital signal. The air-gap malware controls the internal resources of the air-gapped PC, such as the CPU and RAM, enabling it to produce electromagnetic, optical, auditory, magnetic, vibration, or temperature signals that may be utilized to convey the encoded data. A device that is able to collecting data transferred from the sealed with air PC is positioned inside the permitted information transfer range in an outside network. To evade user or administrator observation, the receiver device gets a secure network signals from a near proximity or a concealed location. The received data is then decoded and restored by the receiving device.

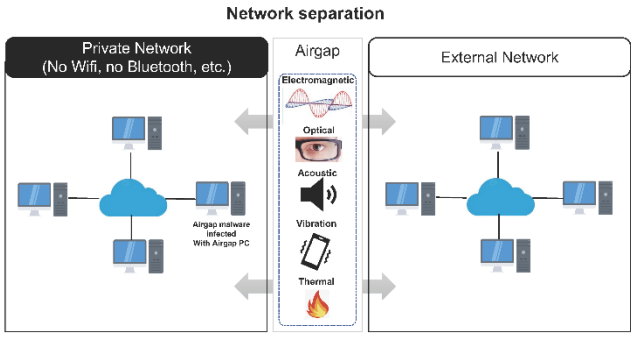

Fig.8. Air-Gap attacks [24a]

Figure 8 depicts the air-gap assault environment.
In this paper, we define the following assumptions and preconditions for conducting an air-gap attack:

- Bluetooth, Wi-Fi, and various other wireless communication technologies are not utilized to link computers in the closed network.
- The air-gap malware is thought to have invaded the closed network through a supply chain attack (SCA) or social assault and effectively attacked an air-gapped PC.
- It is believed that no variables may disrupt data transmission among the sender (i.e. networks) and the recipient (such as external network) employed in the air-gap attack.

5. Fraud Detection Technologies (FDT)

Because many financial companies monitor current fraud strategies using detection rules, fraud approaches that aim to circumvent such rules-based detection mechanisms have gotten more complex. As a result, this is ongoing development on fraud detection systems as depicted in Figure 9.

Fraud detection methods includes not just statistical methods and rules-based identification methods, but also systems that leverage predictable trends in which client transactional attributes are modelled and aggregated via classification procedures. Whenever a transaction behaviour differs from the features of the group that is input, it is flagged as fraudulent based on the degree of departure [25]. Other research on prevalent trends depends on behavioural pattern analysis using artificially intelligent (AI) techniques like the use of machine learning (ML) and data mining.

Statistics-based technology for detection is classified as

1. Processing of data approaches in the context of big databases
2. Methods for calculating and comparing statistic variables.

Various statistics identification of fraud approaches is offered based on the features of the individual sectors of implementation, including credit card, laundering funds, network breach detection, and healthcare and scientific fraud detection [26].

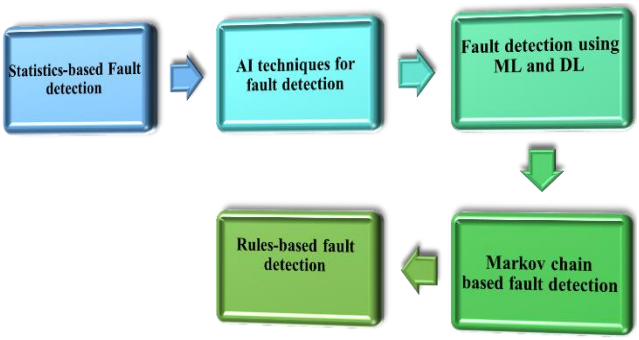

Fig. 9. Various FDT

AI techniques for detection are classified into three types: data mining, pattern identification, and machine learning (ML). Among them is information-mining-based detection technology, which uses data categorisation to automatically categorise anomalous and normal transactions. Representative strategies examined in earlier research in the area of data-mining-based fraud detection includes sequential pattern algorithms employing neural networks with artificial intelligence and Bayesian modelling.

The random forest, SVM, hidden Markov model, deep learning, and other machine learning techniques are examples. Pattern detection, abuse detection using a state transition analysis model, anomaly detection using supervised and unsupervised analysis models, and so on are examples of detection approaches. The gathered financial transaction information is labelled as fraudulent or non-fraudulent, and it is decided if a newly entered transaction is fraudulent or non-fraudulent.

Most financial institutions use rules-based detection of fraud technology, which has an elevated rate of false positives and hence requires a significant amount of labour and time. The Markov chain approach predicts the state transition of consecutive events. Srivastava and Kundu [27] introduced the HMM approach for identifying fraud with credit cards by profiles and analysing the general trends across all users' historical transactions sequences. Even while Markov chain models are extensively employed to depict user activity patterns, but fail to perform well when user behaviour varies [28]. As a result, in the case of internet banking, wherein the level of transition cannot be consistent, the ability to identify fraud performance is generally weak. In accordance with a review article [29], the majority of study articles and publications on data mining techniques linked to banking frauds have studied the application of clustering and classification algorithms, with only a few investigations examining regularities related to financial transaction activities.

6. Discussion

The development of FinTech in fields such as mobile the web, massive amounts of data, cloud computing, online searches, and blockchains has had a significant impact on the financial services industry and forced traditional institutions to modernize. The so-called "AI effect" shows how, as robots become more capable, many tasks that were formerly thought to need "intelligence" end up not requiring it. It is known that keyboard acoustic SCA may exploit audible output from keystrokes to infer the usernames, passwords, or PINs that were input.

Despite the fact that researchers are constantly working to improve acoustic SCA, little has been done to develop a functional defense mechanism against these kinds of attacks. Experts have tried to increase effectiveness by using a variety of methods and attack vectors, such as triangulation, or keypad geometry, extraction of features, and categorization. This paper looks at the security flaws and threats associated with online banking. It also provides a full examination of side-channel assaults (SCA), which are new to digital banking in the age of AI. The report also discusses current research problems and potential directions in the future.

7. Conclusion

In today's environment, the introduction of artificial intelligence (AI) and automation is gradually reducing the demand for electronic banking and payment methods, while making transactions without cash and digital platforms in FinTech's more popular. While such offerings are useful to customers, they do represent severe security risks owing to keyboard side- channel attacks. Keypad security vulnerabilities have evolved as a result of attackers combining current attack tactics with new attack approaches while creating new harmful programs. The goal of this study is to provide improved user authentication techniques by analyzing the safety of data input through a keyboard-based device for authentication of users, particularly Internet banking services. If the authentication data entered through the keyboard device is accessible throughout authentication by the user, attackers may try to illegally login or, worse, steal the victim's money. As a result, the novel keyboard-attack strategies known in the digital banking industry are examined in this research, and the acoustic Side-Channel Attack Mitigation approaches are addressed.

8. References

[1] McCarthy, John; Minsky, Marvin; Rochester, Nathan; Shannon, Claude (1955). "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence". Archived from the original on 26 August 2007. Retrieved 30 August 2007.

[2] Suchismita Gupta, Bikramjit Sarkar, Subhrajyoti Saha et al. A Novel Approach Toward the Prevention of the Side Channel Attacks for Enhancing the Network Security, 20 September 2022, PREPRINT (Version 1) available at Research Square [https://doi.org/10.21203/rs.3.rs-2074983/v1]

[3]Randolph, M.; Diehl, W. Power Side-Channel Attack Analysis: A Review of 20 Years of Study for the Layman. Cryptography 2020, 4, 15.

[4] Mehdiabadi, A.; Shahabi, V.; Shamsinejad, S.; Amiri, M.; Spulbar, C.; Birau, R. Investigating Industry 5.0 and Its Impact on the Banking Industry: Requirements, Approaches and Communications. Appl. Sci. 2022, 12, 5126. https://doi.org/10.3390/app12105126

[5] David, L.; Kaulihowa, T. The Impact of E-Banking on Commercial Banks' Performance in Namibia. Int. J. Econ. Financ. Res. 2018, 4, 313–3

[6] Meher, B.K.; Hawaldar, I.T.; Mohapatra, L.; Spulbar, C.; Birau, R.; Rebegea, C. The impact of digital banking on the growth of Micro, Small and Medium Enterprises (MSMEs) in India: A case study. Bus. Theory Pract. 2021, 22, 18–28.

[7] Panda, S.; Liu, Y.; Hancke, G.P.; Qureshi, U.M. Behavioral Acoustic Emanations: Attack and Verification of PIN Entry Using Keypress Sounds. Sensors 2020, 20, 3015. https://doi.org/10.3390/s20113015

[8] Kuhn, M.G.; Anderson, R.J. Soft tempest: Hidden data transmission using electromagnetic emanations. In Proceedings of the International Workshop on Information Hiding, Portland, OR, USA, 14–17 April 1998; pp. 124–142.

[9] Qiao, H.; Liu, Y.; Yang, A.; Hancke, G. Preventing overshadowing attacks in self-jamming audio channels. IEEE Trans. Dependable Secur. Comput. 2018.

[10] Friedman, J. Tempest: A signal problem. NSA Cryptologic Spectr. 1972, 35, 76.

[11]Loughry, J.; Umphress, D.A. Information leakage from optical emanations. ACM Trans. Inf. Syst. Secur. (TISSEC) 2002, 5, 262–289

[12]Murdoch, S.J.; Drimer, S.; Anderson, R.; Bond, M. Chip and PIN is Broken. In Proceedings of the 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 16–19 May 2010; pp. 433–446.

[13]Anderson, R.; Murdoch, S.J. EMV: Why payment systems fail. Commun. ACM 2014, 57, 24–28.

[14]Bond, M.; Choudary, O.; Murdoch, S.J.; Skorobogatov, S.; Anderson, R. Chip and Skim: Cloning EMV cards with the pre-play attack. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 18–21 May 2014; pp. 49–64.

[15] Shumailov, I.; Simon, L.; Yan, J.; Anderson, R. Hearing your touch: A new acoustic side channel on smartphones. arXiv 2019, arXiv:1903.11137

[16] Yu, J.; Lu, L.; Chen, Y.; Zhu, Y.; Kong, L. An indirect eavesdropping attack of keystrokes on touch screen through acoustic sensing. IEEE Trans. Mob. Comput. 2019.

[17] Zhou, M.; Wang, Q.; Yang, J.; Li, Q.; Jiang, P.; Chen, Y.; Wang, Z. Stealing Your Android Patterns via Acoustic Signals. IEEE Trans. Mob. Comput. 2019

[18] Kocher, P.C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 1996; pp. 104–113.

[19]Kocher, P.; Jaffe, J.; Jun, B. Differential power analysis. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 15–19 August 1999; pp. 388–397.

[20] Genkin, D.; Shamir, A.; Tromer, E. RSA key extraction via low-bandwidth acoustic cryptanalysis. In Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2014; pp. 444–461.

[21] Chandrashekar, A.; Kumar, P.V.; Chandavarkar, B. Comparative Analysis of Modern Mobile Operating Systems. In Proceedings of the 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 6–8 July 2021; pp. 1–7.

[22] Mahor, V.; Pachlasiya, K.; Garg, B.; Chouhan, M.; Telang, S.; Rawat, R. Mobile Operating System (Android) Vulnerability Analysis Using Machine Learning. In Proceedings of the International Conference on Network Security and Blockchain Technology, Huaihua City, China, 15–17 July 2022; Springer: Berlin/Heidelberg, Germany, 2022; pp. 159–169.

[23] Senanayake, J.; Kalutarage, H.; Al-Kadri, M.O.; Petrovski, A.; Piras, L. Android source code vulnerability detection: A systematic literature review. ACM Comput. Surv. 2023, 55, 1–37.

[24]Muhammad, Z.; Anwar, Z.; Javed, A.R.; Saleem, B.; Abbas, S.; Gadekallu, T.R. Smartphone Security and Privacy: A Survey on APTs, Sensor-Based Attacks, Side-Channel Attacks, Google Play Attacks, and Defenses. Technologies 2023, 11, 76. https://doi.org/10.3390/technologies11030076. **[24a].** Park, J.; Yoo, J.; Yu, J.; Lee, J.; Song, J. A Survey on Air-Gap Attacks: Fundamentals, Transport Means, Attack Scenarios and Challenges. Sensors 2023, 23, 3215. https://doi.org/10.3390/s23063215

[25] Bolton, R.J.; Hand, D.J. Unsupervised Profiling Methods for Fraud Detection. In Proceedings of the Credit Scoring and Credit Control VII, Edinburgh, UK, 5–7 September 2001.

[26] Bolton, R.J.; Hand, D.J. Statistical fraud detection: A review. Stat. Sci. 2002, 17, 235–249.

[27] Srivastava, A.; Kundu, A.; Sural, S.; Majumdar, A. Credit card fraud detection using hidden Markov model. IEEE Trans. Dependable Secur. Comput. 2008, 5, 37–48.

[28] Zheng, L.; Liu, G.; Yan, C.; Jiang, C. Transaction Fraud Detection based on Total Order Relation and Behavior Diversity. IEEE Trans. Comput. Soc. Syst. 2018, 5, 796–806.

[29] Ngai, E.W.; Hu, Y.; Wong, Y.H.; Chen, Y.; Sun, X. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decis. Support Syst. 2011, 50, 559–569.