International Journal of Scientific Research & Engineering Trends
Volume 8, Issue 1, Jan-Feb-2022, ISSN (Online): 2395-566X

Fraudify: A Secure Open Banking Platform

Debasis Chakraborty
CEO, Fintract Global Ltd.
London, UK
debasis.chakraborty@fintractglobal.com

Surya Suresh
Data Science Associate, Fintract Global Ltd.
University of Hertfordshire, UK
surya.suresh@fintractglobal.com

Abstract-Fraudulent Activity is a major problem faced by many fields mainly in financial sector. The fraud transactions are performed to buy goods without paying, to get unauthorized access to account and transfer money with account holder's acknowledgement. Ensuring secure authentication can prevent the system from security breaches. Behavioral Biometrics has increasing demand in digital industry as it helps identify the original user and fraudsters by analyzing the behavior that a person possesses. The project incorporates the traditional authentication such as personal identification number along with different advanced biometric authentication such as face recognition, keystroke dynamics, mouse dynamics and geographic location acts like a strong filter to identify the original user to access the system.

Keywords- Authentication, Behavioral Biometrics, Keystroke Dynamics, Mouse Dynamics, Face recognition, G Security Breaches.

I. INTRODUCTION

The digital economy is expanding at a rapid pace. Once relegated to the realms of science fiction, e-commerce, mobile payments, digital wallets, contactless payments, and the internet of things (IoT) are now routine. Social distancing and stay at home orders in response to COVID-19, combined with pandemic related fears over the use of cash have indeed accelerated the shift to digital payments. With radical shift towards digital platform in financial sector, it has become equally important and challenging to ensure the security as it has become topmost sector to face cybercrimes.

The growth in cybercrime coupled with proliferation of digital economy is as close as it can get to a death-knell, if not dealt appropriately. Several security breaches such as Phishing, Malware, mobile spoofing, cloning, and fraud attacks are occurring each day mostly in the financial service sector as it holds the most sensitive data in the virtual world. Challenges that are faced by institutions and customers mainly revolve around authentication, real time analysis and behavior identification. The online identity fraud cost has increased from billion to trillion dollars in recent years. So the organizations spent large resources and working hours to ensure the security, verify customers' identity, detect fraudulent activities and protection from all types of security breaches.

The identity theft and account takeovers are turning out to be easier to perform as there is huge amount of personal data available in the online platform. So, there is increase in demand for Multi-factor Authentication (MFA) to ensure high security against the risk faced in online banking system. Several authentication factors are incorporated to ensure the consumers identity and detect fraud activities. Traditional authentication features like Personal Identification number (PIN) and unlock pattern has been widely employed in many applications for authentication purpose and has become very vulnerable towards digital attacks. To overcome these setbacks, several biometric recognition methods are developed and deployed which can authenticate the user based on the data uniquely available to the user such as users' face, fingerprint, or voice data.

Fraudify is a new market disruptive security method, where the focus is on continuous context-based authentication, which can enhance the user experience and significantly drop the fraudulent activity banks have to tackle. The proposed project is developed after analyzing our competitors and markets, globally and other factors impacting our solution, which showcases that our product is one of its kind that incorporates advanced technologies such as machine learning, multiple authentications etc. to deliver a high-end product addressing the problem holistically for individual users and banks.

The high-level security is achieved by incorporating both static authentication factors and dynamic authentication factors. The behavioral biometrics such as keystroke dynamics and mouse dynamics along with face recognition, location data and password is required during authentication.

II. RELATED WORK

The organizations in financial service sector of all sizes are fighting against different types of security breaches. This is due to the large amount of sensitive data it holds in the digital space which has created opportunities for both consumers and fraudsters to exploit these faceless

© 2022 IJSRET

channels. Merchants face a basic difficulty in controlling risk and preventing fraud while maintaining the high level of customer service that their customers expect [6].

This is exacerbated by the fact that fraud attempts continue, and the dollar amount of fraud has climbed by 12% in the last year, according to Forter's Fraud Attack Index's seventh edition [6]. According to a recent RSA analysis, more than 30% of online banking fraud is perpetrated by criminals using the accounts of purportedly legitimate clients. Providing high level security prevents fraud activities to take place to a certain level. There are many studies on finding new ways to tackle these issues and built a secure and user-friendly channel for digital transactions.

Kiljan et al. review the authentication and communications protocols for online banking adopted by 80 banks worldwide [9]. This study provides an analysis of the temporal evolution of MFA protocols adopted by banks, together with a classification of the incorporated authentication factors and MFA protocols [9]. Althobaiti evaluates the security and usability of MFA protocols based on questionnaires and field tests. The survey focusses on the security of MFA protocols perceived by users [11]. An applied mathematician named Karl Pearson studied biometric research at University College London in the early twentieth century.

Through his research into statistical history and correlation, achieved significant advances in the field of biometrics. The method of moments, the Pearson system of curves, correlation, and the chi-squared test are his historical contributions [5]. Regulators are increasingly pushing for more robust multi- factor authentication systems that require users to confirm their identity. Consumer demand for biometric authentication appears to be on the rise, with a Visa survey released in January 2020 revealing that 52 percent of people would switch banks if their bank did not offer biometric authentication in the future [7,8].

In the field of security research, behavioral biometrics is gaining popularity. This kind of biometric includes keystroke, touch, and mouse dynamics. In on-line courses, keystroke dynamics is already employed as a technique of continual authentication. Keystroke data, on the other hand, could include sensitive information like passwords and usernames. Mouse dynamics data, on the other hand, do not include any sensitive information. As a result, gathering and using this type of data for intrusion detection in online banking systems, is effortless.

User identification during sessions, not just during a login phase, could benefit from keystroke dynamics. According to studies, users with sufficient data can be reliably identified even without the need of usernames and passwords. The Rand report from 1980, which was motivated by individual distinct rhythms when sending telegraphs, was a groundbreaker in keystroke dynamics research. While the telegraph key was used as an input device back then, today's input devices include the computer keyboard, mobile keypad, and touch screen. Garcia's patent from 1986 described a system that required users to type their names for authentication.

Later, Young and Hammon were granted a patent for their description of a keystroke authentication system. The use of keystroke latencies and keystroke pressures as essential metrics of keystroke behavior is mentioned in this patent. Researchers began devising trials to make keystroke dynamics a more realistic tool after the first investigations revealed that keystroke authentication was possible.

Mouse dynamics is a behavioral biometric developed at the University of Victoria's Information Security and Object Technology (ISOT) research group in 2003. User identification in the online browsing process using only mouse clicks was reported by Chuda, Kratky, and Tvarozek in which they reported 96 percent user identification accuracy on a data set containing data with features extracted from 100 clicks of 20 users [14]. For user authentication, Zheng et al. and Hinbarji et al. used mouse movement curves as the basic modelling unit. Using features taken from 100 mouse curves, they were able to get 9.8% EER (approximately 5.6 minutes length mouse data). The trials were carried out on a data set of ten users [15, 16].

Studies prove that the keystroke dynamics and mouse dynamics are two technologies that complement each other [18]. Different authentication factors such as username, password, location and other behavioral biometric data incorporated together would result in highly secure platform for online communication and transaction. Consumers are open and willing to bear some level of friction all through the onboarding process, according to Javelin Strategy and Research's 2021 Identity Fraud Study: Shifting Angles. In exchange, customers expect more secure, ongoing identity identification and protection in their business dealings with a company [13].

III. PURPOSE

With the world entering the post-COVID stage, enhancing fraud detection and prevention techniques has become a necessity for businesses to sustain because frauds are becoming more prevalent and complicated and businesses struggling to incorporate effective and efficient Fraud Detection Systems. With intruders coming up with clever ways to hack systems and get into bank accounts, it becomes very crucial for a sophisticated system that can effectively prevent such attacks. And such a sophisticated system is Fraudify.
Fraudify aims to offer banking institutions a secured fraudulent transaction detection system with high end

© 2022 IJSRET

performance using biometrics namely facial recognition, keystroke dynamics, location, and touch dynamics. The combination of the above mentioned metrics gives users a unique identification that can help them have a safe online banking experience.

Technological advances and innovation drive the evolution of the digital economy. Businesses and financial institutions are expanding their digital offerings and outsourcing fraud detection services to meet customer expectations and stay competitive.

Hence it indeed becomes increasingly necessary for companies to form partnerships and share data to follow traditional non-agile processes towards cyber-security.

IV. PROPOSED WORK

Fraudify uses behavioral biometrics such as keystroke dynamics and mouse dynamics in combination with username, password, face recognition and geographical location (latitude and longitude) to authenticate the user. Of course, this information is taken from the user during the registration process. In addition to this the proposed work also has a bank or admin dashboard that displays various statistical information of the different users that are logging in, their flags (discussed below), account name. Country wise statistics are also shown based on flags.

Using the behavioral biometrics serves the purpose of giving a unique identity to the user thereby preventing any intruder from accessing the online bank account. Behavioral biometrics analyzes a user's digital physical and cognitive behavior and is most commonly used today as a fraud prevention solution.

Behavioral biometrics distinguishes between legitimate users and cybercriminals and identifies people by how they behave and interact online rather than by static information or physical characteristics, like what they know or what they have access to. Why do we need a new way to distinguish between cybercriminals and users online? First, it has become far too easy for cybercriminals to find, steal, or purchase personal data such as email and physical addresses, phone numbers, birth dates, and other personally identifiable information to gain access to or open a fraudulent account.

Second, malware, remote access tools and other technologies used by cybercriminals have exposed the weaknesses of passwords, device ID, one-time passcodes and other authentication tools when taken on their own. Finally, as digital experience has taken center stage, fraud prevention technology must work to introduce a frictionless journey for a majority of good users.
Behavioral biometrics solves these problems by leveraging machine learning to analyze patterns in human activity and detect whether someone really is who they claim to be when they interact online and whether the activity is driven by a human or part of an automated attack. The two kinds of behavioral biometrics that have been used are;

1. Keystroke Dynamics:
The way in which a user types on a keyboard or a touchscreen keypad provides a unique and identifiable behavioral biometrics trait. The input parameters that are taken from the user are uptime key, down time key etc.

2. Mouse Dynamics:
Mouse dynamics address the user authentication problem by verifying the genuineness of a user on the basis of their mouse handling style. This includes the coordinates of the screen mouse that is hovered over, mouse clicks etc. The input parameters that are taken from the user are the X and Y coordinates of the screen within a 10 second time period by adding 10 hidden fields on different parts of the screen.

V. SYSTEM ARCHITECTURE

The key entities included in fraudify are:

1. Register Page:
This page collects the username, account number, password (which has to be a combination of lowercase letters, uppercase letters, special characters and numbers), address, phone number, hint question and the user isrequired to upload a picture of theirs by turning on the camera and clicking a picture.

The keystroke dynamics are collected for the password and the mouse dynamics are collected as usual. The image uploaded goes through a basic image checking script that makes sure that the image being uploaded is not entirely blacked and the user's face is visible. If the image is fine, the user gets successfully registered.

2. Login Page:
This page firstly asks the user permission to turn their location on and permission to turn their camera on. The page collects the user email, password, the user's image and their location. The keystroke dynamics and the mouse dynamics are recorded as well.

- This face image, keystroke and mouse dynamics goes through AI algorithms that help us authenticate the user. The user is also flagged during this process.
- If the keyboard dynamics, mouse dynamics, location and face matches then green flag.
- If location passes, face passes; either the behavioral pattern fails - orange flag - 6 digit email OTP.
- If location fails and any other or all fails - Red flag - 4 digit OTP sent to mobile + last four digits of account.

3. Bank Admin Page:

© 2022 IJSRET

A page that is accessible only by authorized bank staff can see the users logging in with their flag status, search through the user directory, and see the country wise statistical analysis and the time series analysis of the users. The bank admin logs in through distinguished bank credentials.

The key features are.

3.1 BehavioralBiometrics: It basically is how the user interacts with the system, his keyboard movements such as the time taken to type two keys , whether he's used caps lock or shift to type upper case letters and so on, and his mouse dynamics which is how the user uses the mouse and what part of the screen he uses the most. We are using powerful machine learning algorithms to achieve this.

3.2 Flagging The Users: In addition to the two features, we are also using location and face recognition as additional features. These in combination are used to authenticate the user. If the user is not permitting the location or camera they are flagged red. If the user is permitting the location and camera then they can be flagged green (all four matching) and orange (one of the behavioral biometrics failing). The red users are sent a 4 digit mobile OTP which has to be used with the last four digits of their bank account to authenticate and the orange users are sent an OTP to their email.

3.3 User dashboard and bank dashboard: A user dashboard has the basic features that include making transactions and a bank dashboard gives the live analytics of who has logged in and what they were flagged as and country wise flag analysis.

3.4 Face recognition model: A face recognition model to authenticate the user.

- Blocking user for 24 hours in case of suspicious behavior:
- Blocking the user for 24 hours if
- The password is typed incorrect and the OTP fails.
- Or if the image recognition is failing.
- Or if in case there is an entry in the hidden field.

3.5 Algorithms used for Behavioral Biometrics:

- Boosted Tree algorithm: This algorithm is used for keystroke dynamics. Boosting means that each tree is dependent on prior trees. The algorithm learns by fitting the residual of the trees that preceded it. Thus, boosting in a decision tree ensemble tends to improve accuracy with some small risk of less coverage.
- Fraudify uses Python pickling quite a bit to save and reload models and to share model data between concurrent processes. This generally just works, and you do not need to implement any save/load logic in order to have your algorithm be saved and shareable.

3.6 Algorithm used for Face Recognition:

- Support Vector Classifier (SVC): The objective of a Linear SVC is to fit to the data you provide, returning a "best fit" hyper plane that divides, or categorizes, your data. From there, after getting the hyper plane, you can then feed some features to your classifier to see what the "predicted" class is. This makes this specific algorithm rather suitable for our uses, though you can use this for many situations.
- The frontend of this project is developed using React JS and backend using Django Framework supported by Mongo DB database.

VI. DESIGN CONSIDERATIONS

1. Assumptions and Dependencies:
The authentication part is heavily dependent on user data just as any machine learning/deep learning model and this can with increase of users can become a heavy application with respect to the database and added future features.

2. General Constraints:
With a fraud prevention and detection model that is incorporated with an online banking system of an established bank. It is obvious that only the new data is stored, i.e., the behavioral biometrics of new users who have recently registered are stored.

3. Goals and Guidelines:
A better version of the project is aimed that can tackle all the previous constraints and mitigate dependencies to a certain extent. Constant improvement is always a goal.

VII. CONCLUSION

Identity verification solutions that are both quick and accurate are in high demand. It goes without saying that when it comes to protecting customers against fraud, having a simpler onboarding process isn't always preferable. A multi-layered approach that includes enhanced authenticity verification, sophisticated data usage, and constant behavioral monitoring could provide the financial sector the ability to combat fraud.

The physical human traits are significantly more difficult to falsify than security codes, passwords, or hardware keys, and hence biometric authentication is extremely dependable. Hence Fraudify is a very helpful and effective application in the financial sector ensuring high level security and user-friendly GUI.

The new authentication techniques incorporated in Fraudify produce accurate results than expected. Many more user-friendly features can build into the application in future.

REFERENCES

[1] Margit Antal, ElodEgyed-Zsigmond, Intrusion Detection Using Mouse Dynamics, www.ietdl.org, ISSN 1751- 8644. doi: 0000000000

© 2022 IJSRET

[2] https://www.finextra.com/blogposting/17515/multi-factor- authentication-and-identity-fraud-detection-in-the- financial-services-industry
[3] https://www.nice.com/engage/real-time-authentication/
[4] https://www.finextra.com/blogposting/17515/multi-factor- authentication-and-identity-fraud-detection-in-the- financial-services-industry
[5] Debnath Bhattacharyya1, Rahul Ranjan1,FarkhodAlisherovA.2, and Minkyu Choi3. "Biometric Authentication: A Review", International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, September, 2009.
[6] Gregory D. Williamson GE Money – America's, "Enhanced Authentication In Online Banking", Journal of Economic Crime Management, Journal of Economic Crime Management.
[7] https://thefutureidentity.com/fighting-back-against-digital- identity-fraud/https://usa.visa.com/visaeverywhere/blog/bdp/2020/01/02/banking-on-biometrics-1578003687083.html
[8] S. Kiljan, K. Simoens, D. De Cock, M. Van Eekelen, H. Vranken, "A Survey of Authentication and Communications Security in Online Banking", ACM Computer Surveys 49 (4) (2016) 61:1–61:35.
[9] Ingrid Fadelli, "An evaluation of mouse dynamics for intrusion detection", 2018, https://techxplore.com/news/2018-10-mouse-dynamics- intrusion.html.
[10] M. Althobaiti, Assessing usable security of multifactor authentication, Ph.D. thesis, University of East Anglia (2016).
[11] Robert Prigge, "Protecting Customers from Fraud 2021", 2021; https://www.finextra.com/the-long-read/139/protecting-customers-from-fraud-in-2021
[12] https://www.miteksystems.com/blog/consumer-trust-with- onboarding-authentication
[13] Daniela Chuda, Peter Kratky, and JozefTvarozek. Mouse clicks can recognize web page visitors! In Proceedings of the 24th International Conference on World Wide Web, WWW '15 Companion pages 21–225, New York, NY, USA, 2015. ACM.
[14] Nan Zheng, Aaron Paloski, and Haining Wang, "An efficient user verification system using angle-based mouse movement biometrics". ACM Trans. f. Syst. Secur., 18(3):11:1–11:27, April 2016.
[15] Hinbarjim Z., R. Albatal, and C. Gurrin. "Dynamic user authentication based on mouse movements curves". MultiMediaModeling. MMM 2015. Lecture Notes in Computer Science, pages 1–12. Springer, Cham, 2015.
[16] DwijenRudrapal, Smita Das, AshimSaha, Lalita Kumari, N.Debbarma,"A Study And Analysis of Keystroke Dynamics And Its Enhancement For Proficient User Authentication". 2012 4th International Conference on Electronics Computer Technology (ICECT 2012).
[17] Ahmed Awad E. Ahmed, Issa Traore,"Mouse Dynamics Biometric Technology". Behavioral Biometrics for Human Identification: Intelligent Applications, 2010, doi: 10.4018/978-1-60566-725-6.ch010.
[18] Chao Shen; Zhongmin Cai; Xiaohong Guan; Jialin Wang, "On the effectiveness and applicability of mouse dynamics biometric for static authentication: A benchmark study". 2012 5th IAPR International Conference on Biometrics (ICB), ISSN: 2376-4201.
[19] https://www.coursehero.com/file/67715476/Fraudify-Investor-Deckpdf/
[20] Ahmed Awad E. Ahmed, Issa Traore," Mouse Dynamics Biometric Technology", doi: 10.4018/978-1-60566-725- 6.ch010.

© 2022 IJSRET