International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

FICO Authentication Suite and FICO Identity Proofing

[1]Chethan K.G, [2]K.R Sumana, [3]Rajesh Venkatesan

[1]PG Student
[2]Assistant Professor
[3]Software Quality-Lead Engineer
[1,2]Department of Master of Computer Application, NIE, Mysuru, India
[3]Fair and Isaac Corporation Bangalore, India

Abstract - *The FICO Authentication Suite provides the capability that can be easily deployed or integrated with the FICO's credit, risk, fraud, financial crime and customer engagement solutions that ensures the end-end protection across the customer life cycle. The layered and the risk-based controls ensures the consistent user experience and establishes the manual authentication for the customers to ensure that they communicate with the trusted and also the appropriate organization. The risk-based approach is used to provide protection and user experience, providing easy-to-use, integrated security across the customer lifecycle. It provides the. Better enrolment to the registered customers in an easy and efficient way.*

***Key Words*: Risk Based, credit, fraud, layered, integrated**

1. INTRODUCTION

The FICO Authentication Suite (FAS) gives the additional trust of security with a set of authentication capabilities. The customer is given access to the multifactor, biometric and the behavioral authentication. It gives the very solid approach to verify the legitimate customers. It has various step up actions based on the organizational thresholds. The various options are tokens, OTP, facial recognition and voice biometrics. The FAS provides balanced, risk-based approach to protect the customers trusted integrated security across the lifecycle.

2. Three Phases of Authentication

Biometric Authentication

The biometric authentication provides the voice, fingerprint and the facial recognition with a liveness verification. It is used to identify the spoofing by a fraudster. It prevents the attackers from using a picture or video during the enrollment process, it is often referred to as the liveness test. It makes more secure and robust than the traditional liveness system using the traditional standard video techniques. The client-side biometrics uniquely identify the users for an organization. It allows to create the consistent and the positive experience. It has become essential to detect fraud, financial crime and establish the customer confidence. Initially the user must go through the enrolment which can be either any one enrolment among the three that is the face recognition, voice and fingerprint scan. After the successful enrolment the user is asked to enroll for each of the transaction to validate the transaction.

Behavioral Authentication

The behavioral authentication suite allows to monitor the device and the user behavior to identify any anomalies. It uses the device identification, device telemetry, including the logical access patterns, IP addresses, preferred browsers, geolocation and the authentication history. The user-based authentication such as keystroke analysis analyze what not the user types. The factors that influence behavior of user are latency between the successive keystrokes, fingerprint placement and applied pressure and it allows to construct a user's unique signature.

The advantage or benefit of the FICO's behavioral authentication suite is that, the customer experience goes uninterrupted and other factors ensures the identity confirmation. It also includes the Runtime Application Self-Protection (RASP). It provides the user with various score known as risk

Multifactor Authentication

It includes the most popular methods for authentication, including out of band One-time-password (OTP), security questions, Q/R code, challenge/response, one-time transaction and verification codes. It ensures that end users have the convenient experience, including the rapid enrolment, broad device support and the multi device binding.

It allows to deploy the strong authentication in a cost-effective way. The suite can be deployed seamlessly to provide the comprehensive platform and to support the digital platform enrollment. It provides the multiple path for the intuitive interactions with the customers. It also ensures the accurate, more robust and the secure enrolment.

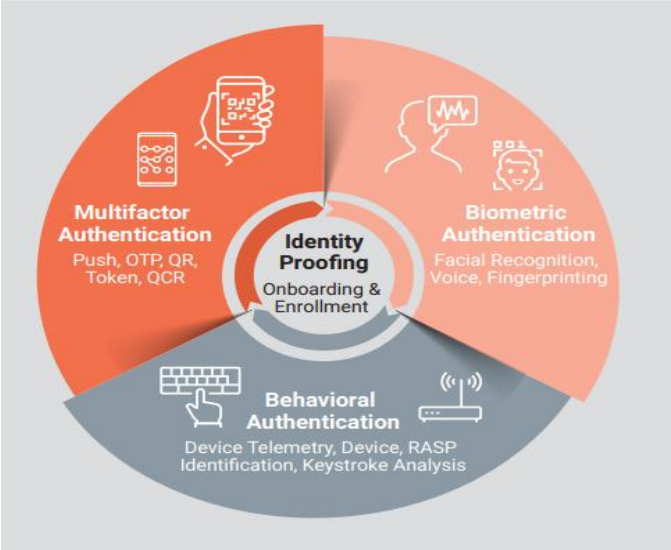


Fig 1. FAS Architecture

Face and Voice Capture

The three major technologies behind the FICO's facial selfie is rather simple but more sophisticated.

Artificial and Machine Learning Capabilities: It is used to determine the subtle differences between the faces in order to prevent the spoofing. Because the faces are vastly different from each other it is difficult to often recognize. Machine learning algorithms are used to overcome the difficulties.

Large sample size for developing a robust facial model: FICO's facial model include millions of faces across the world, to create a model that is both accurate and most robust. It can be difficult because of variations in the tone of a skin colour and also the minimal facial features distinction.

Advanced image and video processing: When the selfie is taken, the imported features of the face are taken by the use of advanced image and the video processing.

Voice Capture

Voice recognition is different when compared to that of the speech recognition, the speech recognition can identify the words, but it fails to recognize the identity of speaker based on the unique vocal attributes of the users.
It mainly consists of two major approaches:

Text independent: It is performed using any spoken phrase or any other speech contents.

Text-dependent: The same phrases used for both the enrolment and verification. Here speaker cannot say anything he likes, to authenticate he needs to speak the predetermined phrase.

3. Literature survey

The paper [1] is based on Restful API's that is needed to trigger the database in the need to RBA and UBA calls that is required to do various behavior and transaction-based process. The API's are called in a sequential manner in order to carry out the smooth transaction. Automation these API's are done in order to quicken the process of transaction and reduce the time taken.

The paper [2] is based on the Junit which is provide additional functionality in the case of testing the functionality of various UI based interfaces such as the action classes, assertions etc. which is required in order to automate and validate the process. It also provides various tags that will helpful to link back the functions together.

The paper [3] is based on the Maven framework which provides the POM (page object model) that is useful in creating the framework separating the both test class and java classes. It helps to easily debug and modify the framework without any difficulties.

Paper [4] is based on the Appium the mobile testing platform for both iOS and android. The Appium is useful in testing the rasp sdk level functionalities. It allows the virtual creation of device in an ease and efficient way allowing various real time application to be tested in an easy and efficient manner.

4. Modules

UBA (User Based Authentication)

The user-based authentication is purely depending on the typing speed or liveliness of the user. The user is trained for five times and his typing characteristics are recorded. Finally, the UBA score is set, and it might be less than or greater than the threshold set for the particular user.

RBA (Risk Based Authentication)

The risk based authentication is purely based on the seven i,e:Device,Browser,Language,IPAddress,Proxy,Geolocation and Time Zone. Whenever these risk elements are changed the risk score keeps on changing. The risk below 800 is acceptable, and if the risk score is above 800 then it will prompt for 2FA.

Risk Scoring

As the foremost layer of the Risk Engine preceding the RBA component, this component is responsible for consuming online banking/session/transaction data provided by the online banking system of financial institutions and producing a risk score to as an indicator of risk. In addition, the risk scoring can also utilize a UBA component in the Risk Scoring Engine whereby the scores derived from the UBA component can be integrated into the calculation of the final risk score as an additional element or factor of risk. The risk scoring collects, evaluates and tracks the history of seven

risk factors with the last factor collected being considered for risk score.

- **Device** - an identifier value set at the domain level as a cookie to detect multiple user accounts logging in from the same browser instance / machine as a simple way to detect fraud.
- **Geo-location** - City, Country obtained from a geolocation database using a known external library.
- **IP Address** - as standard IP Address format.
- **User Agent** - Entire string will be evaluated and historically stored as-is, with user friendly data extracted from the string and stored.
- **Language or Browser Language** - as browser setting

5. EzToken Architecture

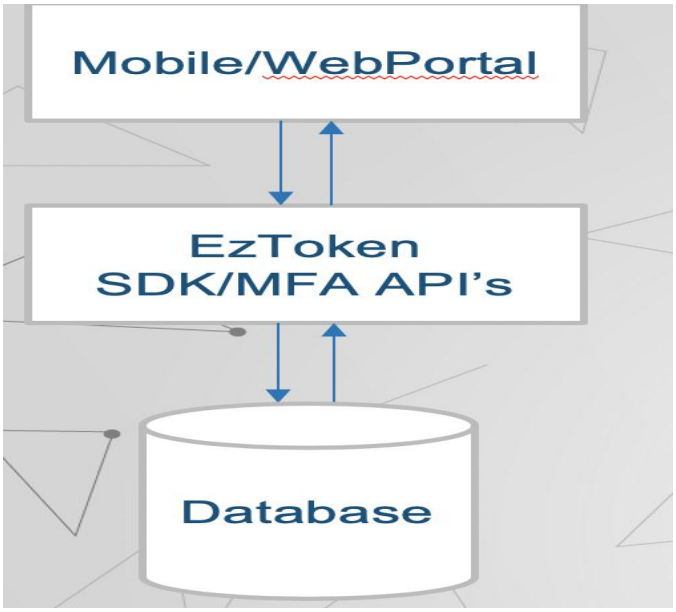
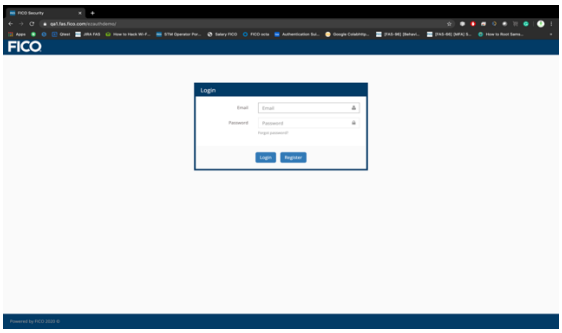


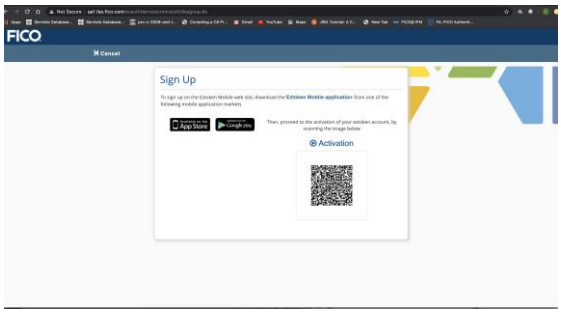
Fig2.Eztoken Architecture

The above figure shows the working of Eztoken app which allows the customer for involve in different enrolment such as face, voice and fingerprint scan. It allows the reliable and fast and secure enrolment that the client finds it very easy to deploy. It allows any one of the enrolments to be active and for getting the one time opt this enrolment comes to validate. In order to access the app, the user must register with valid email address and the activation link will be sent to the mail. On clicking that link the account gets activated and registered. Then the customer will be trained for generating the RBA and UBA score, using keystroke analysis and the risk elements.

6. Results

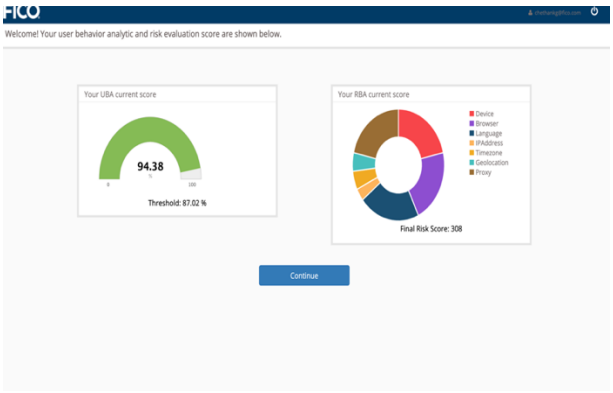


a) Registration page for new user

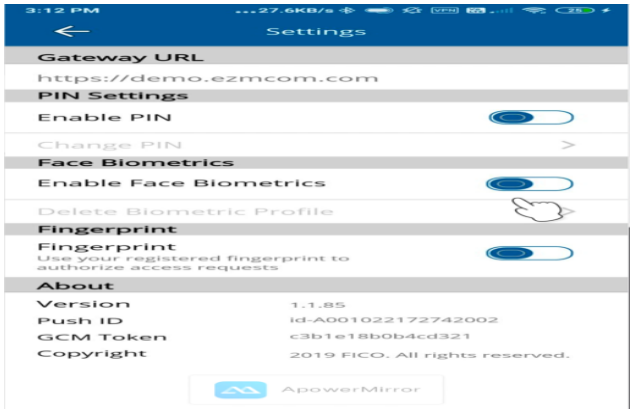


b) Token generated after activating the link

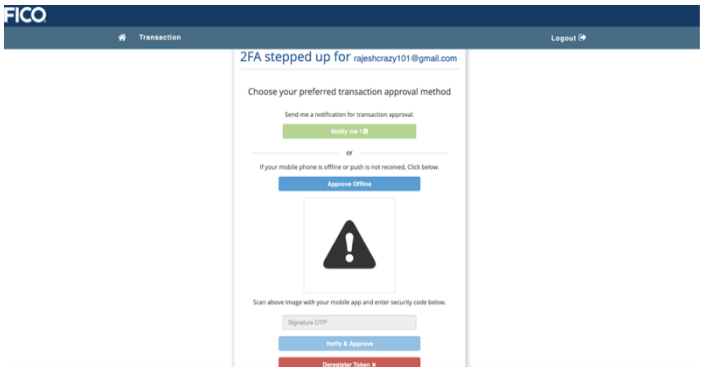
c)Account added after scanning the QR



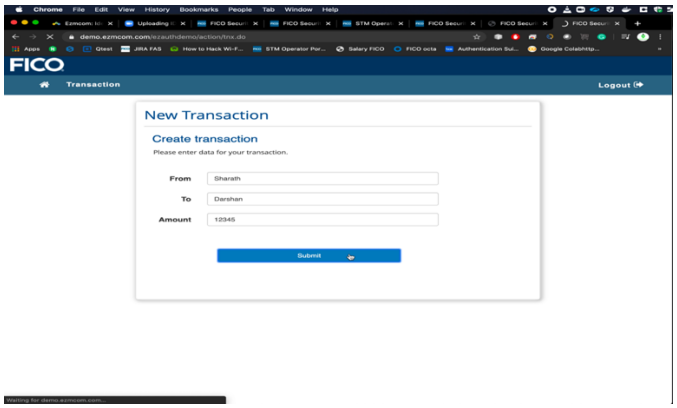
d) UBA and RBA score after training of the user



e) Different enrolment for user



f) 2FA verification



g) New transaction creation

h) Transaction Approval

CONCLUSION

Finally preventing authentication frauds, credit risk, fraud, financial crime, and customer engagement solutions provide layered and risk-based controls and enable a consistent user experience across the enterprise. Pricing norms for multifactor authentication is mature, with a large number of competitors in the market, although relatively small data set of competitive pricing is known. Behavioral and biometric authentication is relatively new with fewer competitors. Market pricing norms are less obvious. EZMCOM pricing was inconsistent from account to account, irrespective of volumes. Used previous pricing as a reference but a bit higher for our standard book pricing. 20-30% discount would equate to similar pricing as before. Standard FICO book pricing does account for regional pricing differentials. ID Proofing pricing is based on competitive intel, equal in pricing Expect FICO standard pricing will be change over the next 6 months as additional competitive data samples are collected.

REFERENCES

1. RESTful API Automated Test Case Generation - Andrea Arcuri Westerdals Oslo ACT, Oslo, Norway and SnT, University of Luxembourg, Luxembourg.

2. Model Based JUnit Testing - Maxim L. Gromov, Svetlana A. Prokopenko, Natalia V. Shabaldina, Andrey V. Laputenko Tomsk State University, Tomsk, Russia.

3. Automatic Updating Method Based on Maven- Xiong Zhen-hai Military Department of Tn formation Management Nanjing Institute of Politics Shanghai, China.

4. Research on Mobile Application Automation Testing Technology Based on Appium - Wang Junmei, Wu Jihong Dalian Neusoft University of Information, Dalian, Liaoning, 116023, China.