International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 08 Special Issue 01 | 2023

Person Data Verification using UIDAIOTP Authentication and Fingerprint Sensor

Prof. P.A.Kharat[1], Mr. Prasad Bhikaji Mali[2], Mr. Soham Vijay Patil[3] , Ms.Shruti Nandakishor Paliwal[4],Ms. Sakashi Shriram Bawaskar[5]

[1,2,3,4,5] *Assistant Professor, Department of Computer Science & Engineering, Padm. Dr.V.B.K.C.O.E.Malkapur, Maharashtra, India*

ABSTRACT

Our System is an Android Application which uses One-time passwords (OTPs) and fingerprints improved by machine learning to verify the uniqueness of people for a particular institute. In order to authenticate their identity, users of the OTP-based systemmust input a code that is transmitted to their mobile phones and entered into thesystem. The device also records the user's fingerprints, which are later compared to a database offingerprints kept by UIDAI. The method can accurately assess if the personis unique or not by spotting patterns and similarities in the fingerprints using machine learning algorithms.The UIDAI system for determining a person's uniqueness has seen a major improvement because to the usage of OTPs, fingerprints, and machine learning. The approach has significantly decreased instances of fraudulent applications and helped keep the Aadhaar system's integrity. Additionally, by learning from past data and enhancing its algorithms, UIDAI has been able to consistently increase the accuracy of the system thanks to the application of machine learning. Overall, the UIDAI system fordetermining an individual's uniqueness has grown to be an essential part of India' national identity programme, offering a trustworthy and safe way to confirm the identityofpersons applying for Aadhar cards

- **Keywords:** Machine Learning, OTP verification, UIDAI, Mobile Appdevelopment.

1. INTRODUCTION

In today’s we live in the society where number of people gather at particular space for particular work like for job, in Society, any function, classes, business meetings and much more. Each institute need to maintain the details of these all peopleswhich comes to their place for certain work. All of them are unknow for the institute but they still need to keep data for the security purpose. But here is the fault in the security system where any person with fake name or identity can enter in the room of such event and may do some unethical work at that workplace which can endanger thelife of all the other people over at work place. Even these can be a great threat for the company as target person may steal some important data and sell it or any hazardous scenario will occur if we allow such random person in the group of people. So, here ouridea is to bring the system which can increase the security level and make it convenient. Current system uses register entries or just word entries to keep details of attendant which can be inaccurate and misleading to the company.

Our system aims to provide the high level of security to such organization where daily random stranger comes for some work examples if there is an interview many random people will come their how can we check that these is the genuine person. It can be used in colleges also for new admissions of random students. So here is our idea wherewe build an Android App which can take user entry along with his Aadhar card whichwill be verified by our app using otp by UADAI site and also figure print of appicatantwill be taken to check uniques. All the details will be stored to institute and only genioun people will get verified in the system. We can keep our data same inside the application. Once the user account is created the user can unlock the app with by his figure prints and can make the direct entry to workplace

2. RELATED WORK

Organizations collect personal data from individuals for various purposes, such as employee onboarding, customer registration, and service delivery. Aadhaar-basedauthentication with OTP is a secure and efficient way of collecting and verifying personal data. This report will discuss the benefits and challenges of using Aadhaar-based authentication with OTP for people data collection in organizations. Aadhaar- based authentication with OTP offers several benefits for people data collection in organizations. Firstly, it is a secure way of verifying the authenticity of an individual's identity as Aadhaar is linked to biometric data, making it difficult to forge or duplicate. Secondly, it is a quick and convenient process as the individual can provide their Aadhaar number and receive the OTP on their registered mobile number, eliminating the need for physical documents. Lastly, it is a cost-effective method as it reduces the need for manual verification and reduces the risk of fraud.

While Aadhaar-based authentication with OTP offers numerous benefits, there are also some challenges associated with its use. Firstly, there may be issues with network connectivity, which can cause delays in receiving the OTP. Secondly, individuals maynot have an Aadhaar number, or their Aadhaar data may not be up to date, causing difficulties in the verification process. Lastly, there may be concerns about privacy and data security, as Aadhaar data is sensitive information that must be protected.

To implement Aadhaar-based authentication with OTP for people data collection, organizations must first register with the UIDAI and obtain the necessary permissions. They must then integrate the Aadhaar authentication API into their data collection systems and ensure that their data collection processes comply with the UIDAI guidelines. Organizations must also ensure that they have adequate data security measures in place to protect personal data.

3. SYSTEM MODEL

The process of person data verification using UIDAI OTP authentication and fingerprint sensors is straightforward. When an individual needs to verify their identity, they provide their Aadhaar number to the verifier. The verifier then sends an OTP to the individual's registered mobile number. The individual enters the OTP and places their finger on the fingerprint sensor. The fingerprint sensor captures the individual biometric data and matches it with the data stored in the UIDAI database. If the data matches, the person's identity is verified.

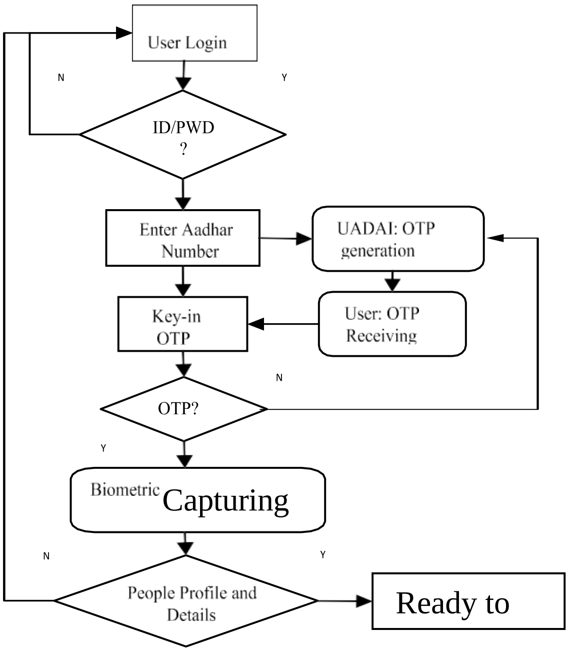

Fig. Data Flow Diagram

BENEFITS:

The use of UIDAI OTP authentication and fingerprint sensors for person data verification has several benefits. Firstly, it is a secure and reliable way of verifying an individual's identity, as biometric data cannot be easily faked or duplicated. Secondly, it is a quick and convenient process, as individuals can

CHALLENGES:

While UIDAI OTP authentication and fingerprint sensors offer numerous benefits, there are also some challenges associated with their use. Firstly, there may be issues with network connectivity, which can cause delays in receiving the OTP. Secondly, some individuals may have difficulty using the fingerprint sensor, particularly if they have a physical disability or a medical condition that affects their fingers' sensitivity. Lastly, there may be concerns about privacy and data security, as biometric data is sensitive information that must be protected.

CONCLUSION:

In conclusion, person data verification using UIDAI OTP authentication and fingerprint sensors is a secure, convenient, and cost-effective way of verifying an individual's identity. While there are some challenges associated with their use, these can be overcome with adequate planning and implementation. As technology continues to evolve, it is likely that we will see further advancements in person data verification methods, and UIDAI OTP authentication and fingerprint sensors will remain an important tool in the fight against identity fraud.

REFERANCES:

[1] Key Pousttchi and Martin Schurig “Assessment of Today’s Mobile Banking Applications from the View of Customer Requirements”

[2] Mohammad Shirali-Shahreza1 and M. Hassan Shirali-Shahreza, “Mobile Banking Services in the Bank Area”, SICE Annual Conference 2007, Kagawa University, JapanSept. 17-20, 2007

[3] 2011.http://en.wikipedia.org/wiki/Mobile_banking, Accessed on Nov 30, 2011.

[4] Hanáçek, P., Malinka, K., Schäfer, J., “e-Banking Security-A Comparative Study”,IEEE Aerospace and Electronic Systems Magazine, 25(1), Pages 29-34, 2010.

[5] Atul Kahate, “Cryptography and Network Security” , McGraw-Hill.

[6] RSA Laboratories (2009), PKCS #11 V2.3 䲢 Cryptographic Token Interface Standard, RSA Security Inc. [7] Housley, R., Ford, W., Polk, W., and Solo, D., “Internet
X.509 Public Key Infrastructure Certificate and CRL Profile”, RFC 2459, 1999

[7] "Agile Methodology," 4 July 2013. [Online]. Available: https://www.codeproject.com/Articles/616070/Agile-Methodology. [Accessed 16April 2017].

[8] P. Jain, "What Makes Java a Powerful Programming Language," 11 February2013. [Online]. Available: https://www.weblinkindia.net/blog/what-makes-java- apowerful-programming-language. [Accessed 16 April 2017].

[9] A. Rongala, "Benefits of Java over Other Programming Languages," 7 May 2015.[Online]. Available: https://www.invensis.net/blog/it/benefits-of-java-over- otherprogramming-languages/. [Accessed 16 April 2017].

[10] "Java SE Downloads," [Online]. Available: http://www.oracle.com/technetwork/java/javase/downloads/index-jsp-138363.html. [Accessed 16 April 2017].

[11] "Android Developers," [Online]. Available: https://developer.android.com/index.html. [Accessed 7 April 2017].

[12] "SoapUI," [Online]. Available: https://www.soapui.org/. [Accessed 31 March2017].

[13] "Crashlytics, Fabric," [Online]. Available: https://fabric.io/kits/android/crashlytics/features. [Accessed 10 April 2017].