IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

Active Authentication on Mobile Device using Stylometry

Shikha Agarawal[1], Ashwin Gujarathi[2], Abhilash Dhumane[3], Pramil Bhosure[4], Mangesh Vinchankar[5]

[1,2,3,4,5]Dept. of Computer Engineering, All India Shree Shivaji Memorial Society's Institute of Information, Technology, Pune University, Pune, India

Corresponding Author: gujarathiashwin9@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i4.854858 | Available online at: www.ijcseonline.org

Accepted: 20/Apr/2019, Published: 30/Apr/2019

Abstract— Behavioural biometrics takes the authentication one step further, requiring the user to not only have the right fingerprint to logon, but to prove that they are the same person whom they claim to be throughout the duration of the session. This takes into account the way in which a person interacts with a device, such as the force with which they hit a key, the angle they use to swipe a touch screen, or their typing speed. Tracking and analyzing these areas allows users to safely use the same password their behaviour for every login. We need to change the way we think about security across passwords, static and behavioural biometrics. Since virtually every authentication technique can be compromised, user should not rely solely on any single control for authorizing, but adopt a layered approach to security, combining the various available authentication technologies to improve both accuracy and user experience.

Keywords— Android, Sensors, API, SQLite, Java

I. INTRODUCTION

Generally we use password or pattern to unlock our phone but if someone find the password or pattern of your phone it becomes easy to access the phone. Anyone who knows password of the mobile can do unwanted things like sending message to other person from your phone. Hence there is strong need of an application which continuously monitors to authenticate the real user of the mobile using the behaviour of the user like texting speed. A human behavioural pattern consists of a variety of different unique "semi-behaviours"; all mixed together into a larger an utterly more unique profile. Since every person's unique Behaviometric pattern is formed not only by biometric features, like the way you move your hand, but is also influenced by more social and psychological means, like if you are native in the language you write, it is just about impossible to copy or imitate somebody else's behaviour in front of the computer. By continually comparing different aspects of the current input stream with a previously stored user profile. In this application, a mobile user feeds all the necessary information like mobile number, email, Security password during initial authentication. Whenever unauthorized user tries to access the mobile, behaviour of the user is matched with the behavioural data of the real user which authenticates the user. If the data is not matched then system asks security question to user. If the answer is wrong then system restricts all the access to mobile, takes the picture of user via front camera and sends security alerts to the email of the real user. In this way owner of the mobile phone will come to know that someone accessed the mobile without permission. Although the owner of the mobile phone can start and stop the service of our application as per need. Also user can change the behavioural data stored in mobile phone in case change of behaviour like increase in texting speed. Active authentication is an approach of monitoring the behavioural biometric characteristics of a user's interaction with the device for the purpose of securing the phone when the point of-entry locking mechanism fails or is absent. In recent years, continuous authentication has been explored extensively on desktop computers, based either on a single biometric modality like mouse movement or a fusion of multiple modalities like keyboard dynamics, mouse movement, web browsing, and behaviour biometrics. Unlike physical biometric devices like fingerprint scanners or iris scanners, these systems rely on computer interface hardware like the keyboard and mouse that are already commonly available with most computers. In this paper, we consider the problem of active authentication on mobile devices, where the variety of available sensor data is much greater than on the desktop, but so is the variety of behavioural profiles, device form factors, and environments in which the device is used. Active authentication is the approach of verifying a user's identity continuously based on various sensors commonly available on the device. We have studied four representative modalities of stylometry (text analysis), application usage patterns, web browsing behaviour, and physical location of the device. These modalities were chosen, in part, due to their relatively low power consumption. In the remainder of the paper these four

modalities will be referred to as TEXT, APP, WEB, and LOCATION, respectively.

An extra layer of security is important for the safety of data in mobile phones. Hence active authentication adds extra layer of security to the mobile phone to protect the device from unwanted access.

II. LITERATURE SURVEY

[1**]** Decision fusion for multimodal active authentication by Alex Fridman, Ariel Stolerman, and Sayandeep Acharya, Drexel University Patrick Brennan and Patrick Juola, Juola & Associates Rachel Drexel University . They presented the topic Identity verification for access control presents a trade-off between maximizing the probability of intruder detection and minimizing the cost for the legitimate user in terms of distractions and hardware requirements.

[2] Unobtrusive user-authentication on mobile phones using biometric gait recognition by Mohammad O. Derawi , Claudia Nickel, Patrick Bours and Christoph Busch, Norwegian Information Security Lab., Gjøvik University College, Norway Hochschule Darmstadt, University of Applied Sciences (CASED) they proposed the need for more security on mobile devices is increasing with new functionalities and features made available. To improve the device security we propose gait recognition as a protection mechanism.

[3]Active authentication for mobile devices utilizing behavior profiling by Fudong Li, Nathan Clarke, Maria Papadaki,Paul.They proposed system with authentication. DowlandWith nearly 6 billion subscribers around the world, mobile devices have become an indispensable component in modern society. The majority of these devices rely upon passwords and personal identification numbers as a form of user authentication, and the weakness of these point of-entry techniques is widely documented. Authentication using the behaviour of user .

[4] Continuous Verification Using Multimodal Biometrics by Terence Sim, Member, IEEE, Sheng Zhang, Student Member, IEEE, Rajkumar Janakiraman, and Sandeep Kumar They proposed Conventional verification systems, such as those controlling access to a secure room, do not usually require the user to re-authenticate himself for continued access to the protected resource. This may not be sufficient for high-security environments in which the protected resource needs to be continuously monitored for unauthorized use.

[5] Optimal Fusion of Multimodal Biometric Authentication Using Wavelet Probabilistic Neural Network by Ching-Han Chen and Ching-Yi Chen, Department of Computer Science and Information Engineering, National Central University, No.300, Jhongda Rd., Jhongli City, Taoyuan County, TaiwanDepartment of Information and Telecommunications Engineering, Ming Chuan University, Taoyuan, Taiwan, ROC. Proposed In order to enhance security and protection capability, the integration of different biometric features to set up multimodal biometric authentication system is an effective way. It can provide complementary information to enhance recognition rate, and it can further enhance the reliability and stability of the identity authentication system.

[6] Authorship Verification for Short Messages using Stylometry Marcelo Luiz Brocardo, Issa Traore, Department of Electrical and Computer Engineering, University of Victoria - UVIC Victoria, British Columbia, Canada Sherif Saad, Isaac Woungang, Department of Computer Science Ryerson University Toronto, Ontario, Canada. Proposed Authorship verification can be checked using stylometric techniques through the analysis of linguistic styles and writing characteristics of the authors. Stylometry is a behavioral feature that a person exhibits during writing and can be extracted and used potentially to check the identity of the author of online documents.

[7] Security Enhancement of IPV6 Using Advance Encryption Standards and diffle helman is written by Mohammad Amjad which is research paper publish by IJSRNSE in 2017 which contains research regarding the interface ID enciphered by using advance Encryption Standards (AES).To enhance the security cryptographic algorithm Diffle Hellman for authentication and AES algorithm for encryption and decryption process.

[8] Mobility-Based Anomaly Detection in Cellular Mobile Networks by Bo Sun, Dept. of Computer Science Lamar University Beaumont, TX 77710 Fei Yu, Dept. of Electrical and Computer Engineering University of British Columbia BC, Canada V6T 1Z4 Kui Wu, Dept. of Computer Science University of Victoria BC, Canada V8W 3P6 Victor C.M., Leung Dept. of Electrical and Computer Engineering University of British Columbia BC, Canada V6T 1Z4. Proposed This paper presents an efficient on-line anomaly detection algorithm that can effectively identify a group of especially harmful internal attackers - masqueraders in cellular mobile networks. Our scheme is derived from a well-developed data compression technique. We use cell IDs traversed by a user as the feature value.

[9] Anomaly-based Intrusion Detection Using Mobility Profiles of Public Transportation User by Jeyanthi Hall, Michel Barbeau, Evangelos Kranakis Carleton University, School of Computer Science Ottawa, Ontario, Canada K1S 5B6. Proposed This paper examines the feasibility of using profiles, which are based on the mobility patterns of mobile users, who make use of public transportation, e.g. bus. More

specifically, a novel framework, which makes use of an instance based learning technique, for classification purposes, is presented. In addition, an empirical analysis is conducted in order to assess the impact of two key parameters.

[10] A survey of possible attacks on text and graphical password authentication technique is written by Sanjay E. Pate and Bhojaraj H. Barhate which is survey paper publish by IJSRCSE in 2018 which contains survey regarding position based routing protocols which offers significant performance increase over traditional ad hoc routing protocols.

III. SYSTEM ARCHITECTURE

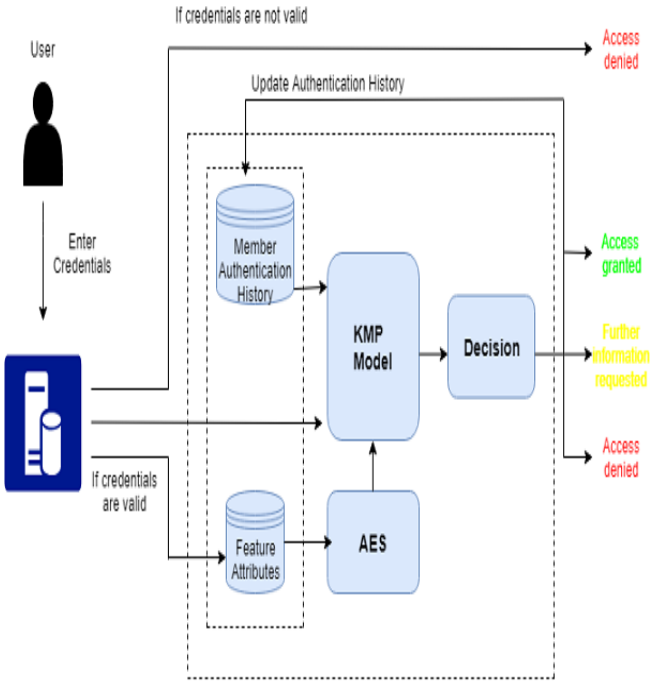


Fig 1: System Architecture

Initially, owner of the mobile device will register on the device with email and mobile number. Once the user is registered, it can login on the application. After user logged in, the service of authentication can be activated and deactivated by the owner of that particular mobile only. Initially user's credentials like typing speed, location details, contact details, network details will be taken as input and stored in database. After authentication service is started, authentication service starts in background and application will keep track of user and match the credentials with the data stored in database. Authentication service can only be disabled by the owner of the mobile using correct email Id and password. If there is any mismatch, application will ask security questions which if answered wrong the security action will be taken.

SEQUENCE DIAGRAM

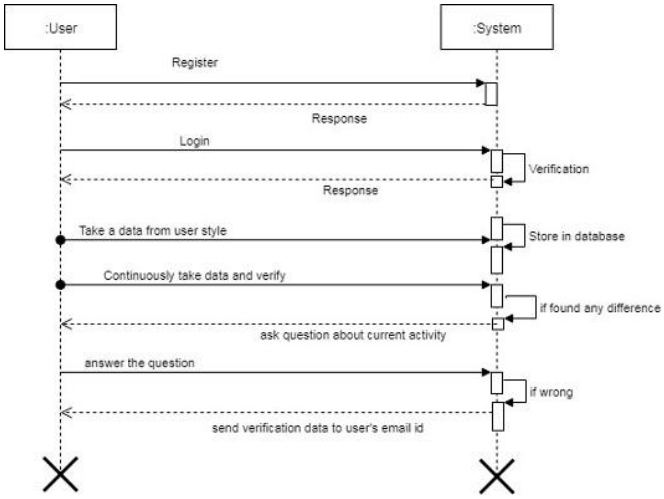


Fig 2: Sequence Diagram

IV. KEY ISSUES

The main issue regarding the application is that it should not be disabled. It will not authenticate the user if application is disabled. Other issues like if application is uninstalled then authentication service will stop.

V. ADVANTAGES OVER OTHER SIMILAR SYSTEMS

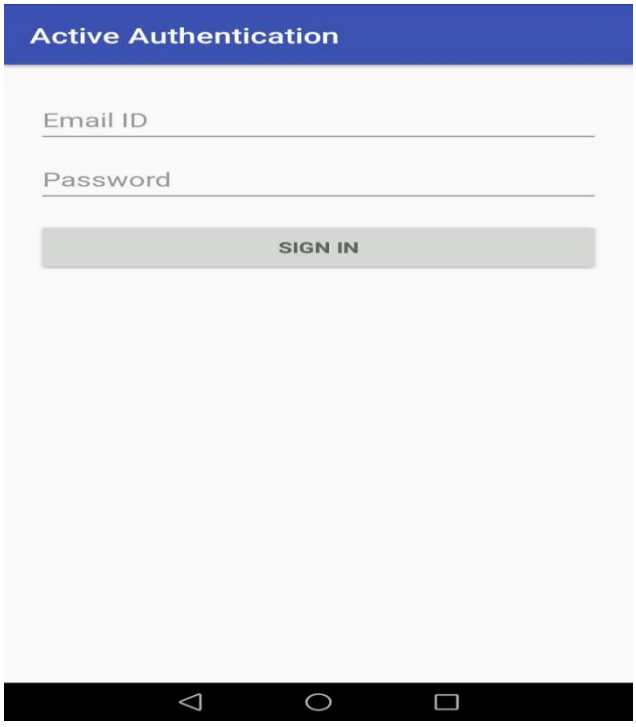
Significant advantage is that it authenticates the user in real time use of mobile devices. This ensures that the one who is operating the device is real owner of the device. Also the service can be stopped at any time and again can be started as per the need of user.

VI. RESULTS

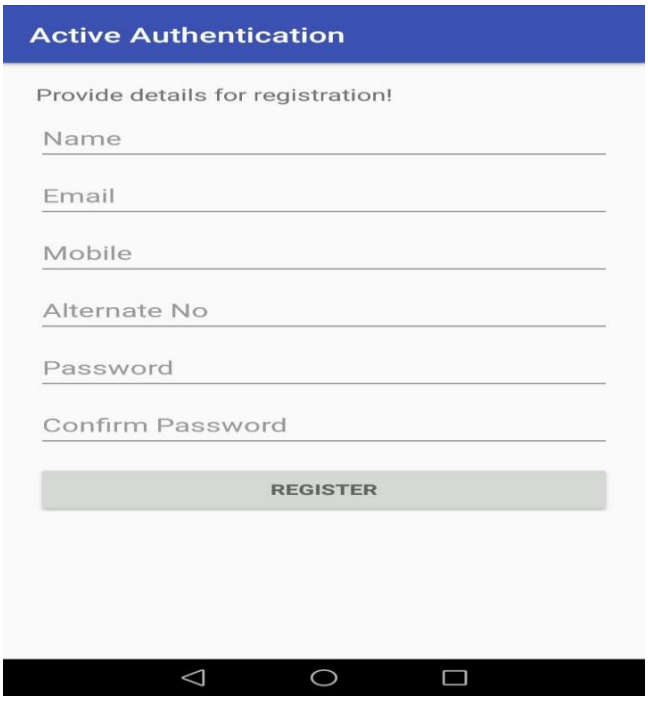
We proposed a system for active authentication on mobile based on four biometric modalities: text, application usage, web browsing, and location. Using this fusion method we addressed the problem of active authentication and characterized its performance on a real-world data set of different subjects, each using their personal Android mobile device for a period of at least few days. The authentication system achieves an equal error rate (ERR) of 0.05 after 1 minute of user interaction with the device. We showed the performance of each individual classifier. The application immediately responds to the unauthorized user once it detects changes in performance.

The results of the project are provided with screenshots as below:

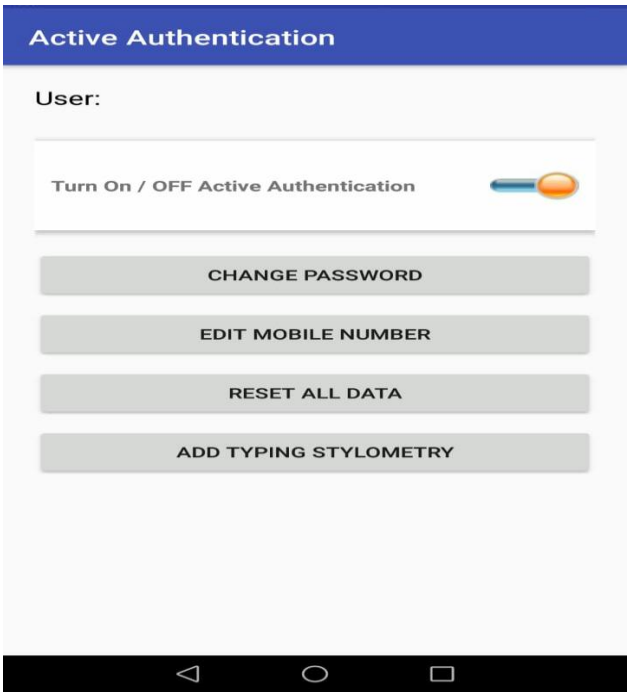
The first screenshot shows the homepage of our project where we register and login.



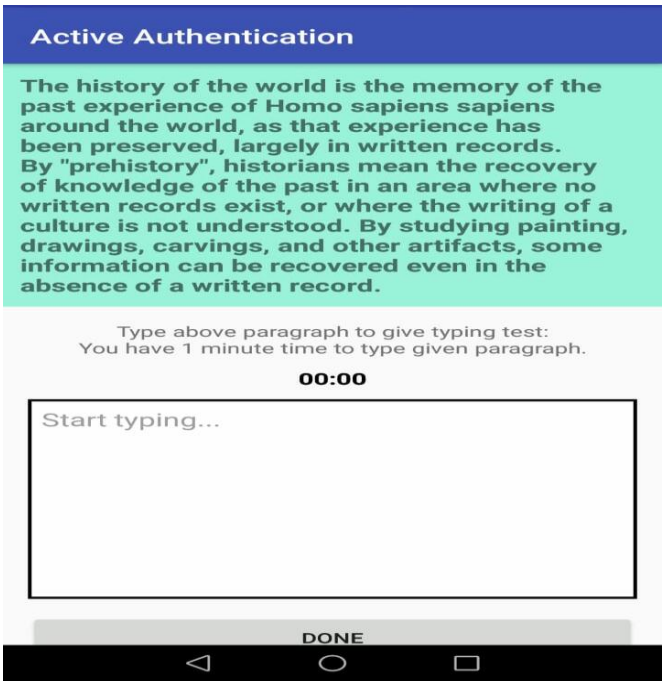
The registration process is very important which required to store the information of authorized user. The mobile number and email Id are required to verify by OTP verification and same are used for security alerts in the application.



Following is the screenshot of the page from where user can activate and deactivate the authentication service. And the page from where user can add typed stylometry.



User has to type predefined paragraph to add his/her stylometry in the system at first time. user can type here to add typing stylometry. user is given one minute to add typing stylometry.



VII. CONCLUSION

Our proposed system uses Android technology which is a mobile application. It authenticates the real user of the particular mobile devices. Our system uses stylometry of the user. With this kind of application we have moved to next step of the authentication of the mobile phone. Our application can be used by any person without any difficulties to use. Our application is easy to use.

VIII. ACKNOWLEDGEMENT

We pay our thanks to Prof. Shikha Agarwal for providing a great support to us. She guided our project team efficiently. We successfully accomplished our work only due to her guidance.

IX. REFERENCES

[1] M. Duggan, "Cell phone activities 2013," Pew ResearchCenter, Washington, DC, USA, 2013.
[2] S. Egelman et al., "Are you ready to lock?" in Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2014, pp. 750–761.
[3] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "Its a hard lock life: A field study of smartphone (un) locking behavior and risk perception," in Proc. SOUPS, 2014, pp. 1–18.
[4] D. Van Bruggen et al., "Modifying smartphone user locking behavior," in Proc. 9th Symp. Usable Privacy Security, 2013, pp. 1–14.
[5] C. Shen, Z. Cai, X. Guan, and J. Wang, "On the effectiveness and applicability of mouse dynamics biometric for static authentication: A benchmark study," in Proc. IEEE 5th IAPR ICB, 2012, pp. 378–383.
[6] A. Fridman et al., "Decision fusion for multimodal active authentication," IEEE IT Professional, vol. 15, no. 4, pp. 29–33, Jul. 2013.
[7] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition," in Proc. IEEE 6th Int. Conf. IIH-MSP, 2010, pp. 306–311.
[8] F. Li, N. Clarke, M. Papadaki, and P. Dowland, "Active authentication for mobile devices utilising behaviour profiling," Int. J. Inf. Security, vol. 13, no. 3, pp. 229–244, Jun. 2014.
[9] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous verification using multimodal biometrics," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 687–700, Apr. 2007. [10] J. Kittler, M. Hatef, R. Duin, and J. Matas, "On combining classifiers," IEEE Trans. Pattern Anal. Mach. Intell., vol. 20, no. 3, pp. 226–239, Mar. 1998.

AUTHOR'S PROFILE

Mr. Ashwin Gujarathi is currently pursuing Bachelor of Computer Engineering from AISSMS's Institute of Information Technology, affiliated to Savitribai Phule Pune University in year 2019. The paper is in his interest of research work in the domain of data security.

Mr. Abhilash Dhumane is currently pursuing Bachelor of Computer Engineering from AISSMS's Institute of Information Technology, affiliated to Savitribai Phule Pune University in year 2019. He has done her research work in data security field as a part of the case study based on the same concept which is represented in the paper.

Mr. Pramil Bhosure is currently pursuing Bachelor of Computer Engineering from AISSMS's Institute of Information Technology, affiliated to Savitribai Phule Pune University in year 2019. As a part of the course curriculum, he chose to work on data security and studied the topic. Based on that, put his research work in the paper.

Mr. Mangesh Vinchankar is currently pursuing Bachelor of Computer Engineering from AISSMS's Institute of Information Technology, affiliated to Savitribai Phule Pune University in year 2019. His interest in the domain of data security made her do some research work and put it in here.

