Efficient Usage On Mobile Device Through Stylometry and Wi-Fi Network

Manibalan.A[1], Syed Ibrahim.N[2], Mrs. Kayalvizhi.S [3],

[1]*Final Year, Computer Science and Engineering, DACE,*
[2]*Final Year, Computer Science and Engineering, DACE,*
[3]*AP, Computer Science and Engineering, DACE,*

ABSTRACT

This paper presents an Android based Application which is a security application. The idea behind this project is to develop an application which will help user of android to create Admin and Guest accounts,Security holes in Android operating system occur due to the permission based security model which is not properly enforced during system design. Permission based security model has central role hence it creates security holes in Android OS.Google's android security model erased by its openness.Different techniques have been developed to ensure the separation of enterprise content and personal data on any device within work premises.Today enterprises has enabled the ability to restrict the third-party applications within working environment.An application restriction policy is configured through mobile application using Application Restriction Manager (ARM).ARM is a Policy Manager that allows an individual to set different constraints for each installed application.

Keyword:Authentication, Admin panel, Security, wampserver, myphpadmin.

I. INTRODUCTION

Smartphoneshaveevolvedrapidlyfromapurevoicecommunication devices to a general purpose mobile computers and personal assistants. Security of mobile devices is becoming more crucial over time

as these devices start to accumulate a lot ofsensitive data about their users, such as emails, calendar,pictures,communicationdata, financialdataandrecently alotofsensordataincludinglocation. Typing a password is still the most common authentication mechanism, which is clearly cumbersome especially on the go. Recently new methods of authentication have been used including finger print recognition, drawing a pattern on screen, or face recognition. While these methods are trying.We consider the real-time application of this technology for active authentication. As a user begins interacting with the machine, the classification system collects behavioral biometrics from the interaction and continuously verifies that the current user has access permission on the machine. This approach adds an extra layer of distraction-less access control in environments where a computer is at a risk of being intermittently accessed by unauthorized users.

These observations motivated the relatively recent interest in combining classifiers. The idea is not to rely on a single decision making scheme. Instead, all the designs, or their subset, are used for decision making by combining their individual opinions to derive a consensus decision. Various classifier combination schemes have been devised and it has been experimentally demonstrated that some of them consistently outperform a single best classifier. However, there is presently inadequate understanding why some combination schemes are better than others and in what circumstances.

We propose to use decision fusion in order to asynchronouslyintegrate the four modalities and make serial authentication decisions. While we consider here a specific set of binary classifiers, the strength of our decision-level approach is that additional classifiers can be added without having to change the basic fusion rule. Moreover, it is easy to evaluate the marginal improvement of any added classifier to the overall performance of the system. We evaluate the multimodal continuous authentication system by characterizing the error rates of local classifier decisions, fused global decisions, and the contribution of each local classifier to the fused decision. The novel aspects of our work include the scope of the dataset, the particular portfolio of behavioral biometrics in the context of mobile devices, and the extent of temporal performance analysis.

II. SYSTEM MODULE

List of modules

- Admin panel creation
- Policy Manager
- Authentication
- Admin restriction system

Admin panel creation:

Develop the admin panel using local host (wampserver & myphpadmin) and create the default login account for all the application user along with restriction menus.

Policy Manager:

The admin can control the android application only if the terms and conditions (policy) are accepted by the android user.

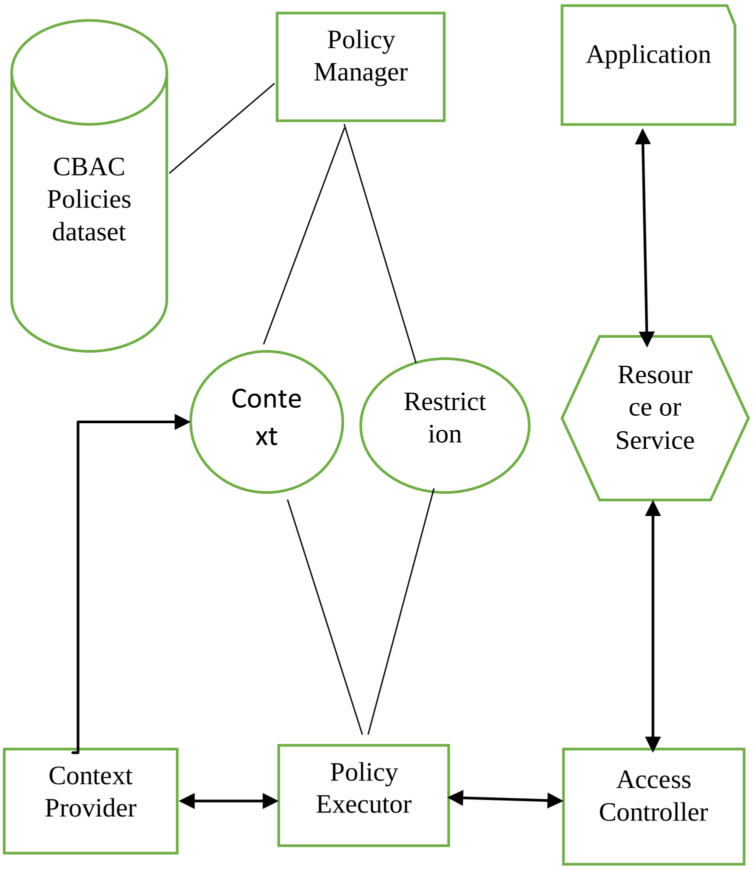
Authentication:

The authentication process will be done between the mobile device & admin panel in the login account if and only if login is successful and gets the user permission to access the admin panel.

Admin restriction system:

If the user login the account in android mobile it will be shown in the admin panel who are logging in &being in online list only then admin can set the privileges for users.

III. ARCHITECTURE DIAGRAM



IV. RELATED WORK

[1] HongLu et al. proposed “Unobtrusive Gait Verification for Mobile Phones “.In this paper, they proposed a gait verification system for mobile phone without any assumption of body placement or device orientation. The main advantage is gait analysis could be used in two types of security tasks: verification and identification. The focus of this paper is primarily on verification, given the assumption that mobile phones are typically personal devices. Our proof-of-concept software demonstrates that it can run on off-the-shelf Android smart phone in real time.

[2] Alex Fridman et al. proposed “Decision Fusion for Multi-Modal Active Authentication”. They proposed a sensor for each modality and organize the sensors as a parallel binary detection decision fusion architecture. The main advantage is feature space is potentially boundless, with frequency measurements or numeric evaluations based on features acrossdifferent levels of the text, including function words, grammar, character n-grams and more The global decision is of better quality (i.e., lower probability of error) than that of the best sensor operating by itself. We are also able to characterize the marginal contribution of each modalityto the overall

FAR/FRR performance. Futureworkwillbegearedtowardopenworldauthenticationon a larger data set with a more expansive portfolio of metrics.

[3]Josef Kittler et al. proposed "On Combining Classifiers" .They proposed an experimental comparison of various classifier combination schemes demonstrates that the combination rule developed under the most restrictive assumptions—the sum rule—outperforms other classifier combinations schemes. The main advantage is Instead of all the designs, or their subset, are used for decision making by combining their individual opinions to derive a consensus decision. The sensitivity analysis has shown that the sum rule is most resilient to estimation errors and this may provide a plausible explanation for its superior performance.

[4]Ching-Han Chen1 et al. proposed "Optimal Fusion of Multimodal Biometric Authentication Using Wavelet Probabilistic Neural Network". They proposed complementary information to enhance recognition rate, and it can further enhance the reliability and stability of the identity authentication system. The main advantage is biometric authentication system is to provide the decision of acceptance (an authorized user) or rejection (a non-authorized user) for the system.All these human face images will be randomly classified as training samples and test samples.

[5]Dirk Van Bruggen et al. proposed "Modifying Smartphone User Locking Behavior". They proposed the security risk is exacerbated by the tremendous heterogeneity of the personal mobile devices and their respective installed pool of applications. Furthermore, by virtue of the devices not being owned by the organization, the ability to authoritatively enforce organizational security polices is challenging. The main advantage is one of the most common basic security approaches is screen locks, which enable a user to protect access to their device by automatically locking the device whenever the screen is turned off .Finally, we believe that the present study opens a wide variety of questions for future work regarding the factors affecting smartphone security behavior.

[6] Ching-Han Chen, Ching-Yi Chen2et al. proposed "Biometric Authentication Using Wavelet Probabilistic Neural Network". They 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. The main advantage is high regonicition rate.After using Sobel filter to enhance the image of iris texture, vertical projection way is used to convert the image to 1-D energy profile signal, then through the use of 1-D wavelet transform, iris feature with high recognition rate can then be extracted . In this research, face feature and iris feature has been associated to form the needed multimodal biometric feature vector [6].

[7] Mattias Andersson, Hironao Okada et al. proposed "Towards Multiple User Active Authentication in Mobile Devices". They proposed interpret this problem in an open-set framework and introduce the notion of probability of negativity to alleviate the effect of multiple users in authentication. The main advantage is text, application usage, web browsing, and location. The key features are the microcontroller (MCU), which activates the various parts of the circuit only when they are needed, and the simple voltage divider used to measure the vaginal resistance of the cow.

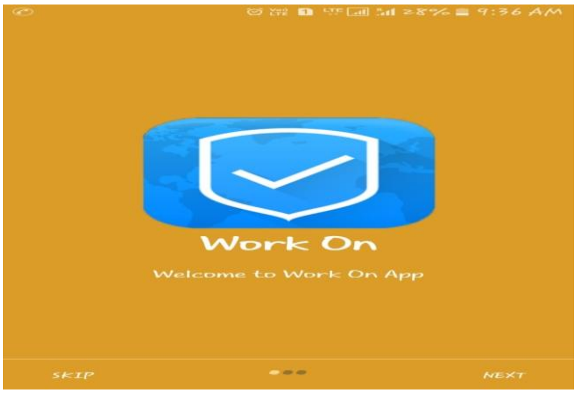
[8] Dr. Sridhar Mandapati, Sravya Pamidi, Sriharitha Ambati et al. proposed “Extracting IM evidence of android apps sign in or purchase”. They proposed the Android dominates the smart phone market (86.2%) and has become pervasive, running in `smart' devices such as tablets, TV, watches, etc. Nowadays, instant messaging applications have become popular amongst smart phone users and since 2016 are the main way of messaging communication. The main advantage is Instant Messaging Application (IMA).The aim of this step is to identify the patterns of the targeted data in multiple memory dumps, acquired in different days and times, in order to create accurate and non-circumstantial regular expressions to match them. The produced regular expressions are optimized with thorough testing to retrieve all the available messages and avoid false positives.

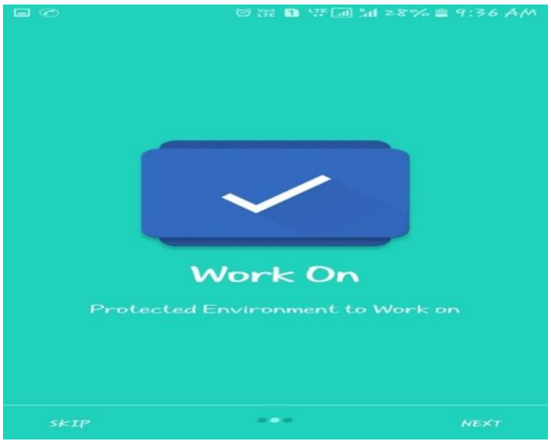
[9] Abdul Hadi H. Nograles, Felicito S. Caluyo et al. proposed “Monitoring Temperature Changes in Body”. They proposed Wireless system was designed to measure body temperature remotely and detect early stage of pregnancy in multiple cows which consists of Personal computer (PC), Xbee modules and MATLAB program. The Xbee transmitters with the LM35 temperature sensors were attached under the tail head of the cows. The main advantage is to increase in temperature was noted if it has at least two standard deviation higher than the mean of the previous three readings and is about 0.46 0C higher. The base station unit is the Xbee Data Terminal Equipment (DTE) board with an Xbee module configured as coordinator provides communication between remote unit or end device that is attached to each cow and PC via radio frequency. Coordinator can receive any data from any Xbee module with the same Personal Area Network Identification (PAN ID).

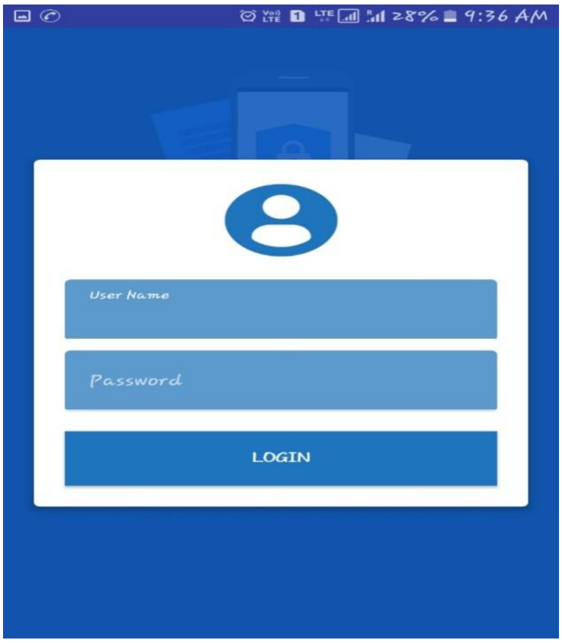
[10] Akshata V.S, Rumana Pathan, Poornima Patil, Farjana Nadaf et al. proposed “Toward Writing Style Anonymization”. They proposed anonymouth, a novel framework for anonymizing writing style. Without accounting for style, anonymous authors risk identification. This framework is necessary to provide a tool for testing the consistency of anonymized writing style and a mechanism for adaptive attacks against stylometry techniques. The main advantage is important to note that Anony mouth is only the first step toward a tool to acheive stylometric anonymity with respect to state-of-the-art authorship attribution techniques. Simply stripping descriptive words, modifying tense, and altering the point of view (e.g. from third to first person) would certainly increase anonymity; though clearly at the expense of the documents impact on the audience (affect). While this is one approach that may be taken, it seems far from ideal, and as though it ought to be considered as a last resort.

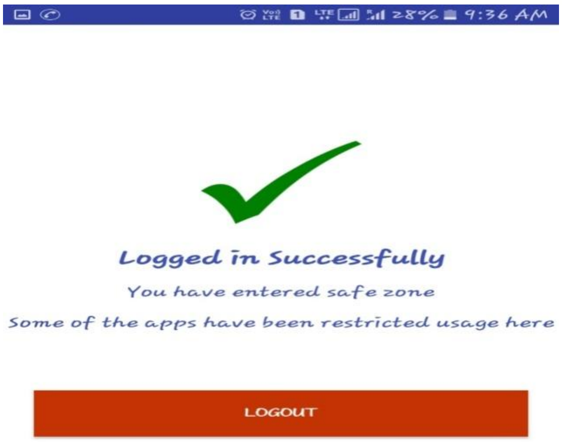
VI. PROPOSED

In our paper, we rely on Wi-Fi-based positioning techniques to retrieve the location of the device. In addition to these techniques, we also collect location data retrieved from GPS and cellular networks for situations where there is no Wi-Fi coverage in the areas of interest. Moreover, we use public GPS location data in defining policy contexts for areas that have not been previously visited, as described in Section In this section, we introduce a brief description on methods used in smart phones for locating the devices. In this section, we introduce the design of our architecture through describing the components of our access control framework with the corresponding role of its entities. Our framework consists of an access control mechanism that deals with access, collection, storage, processing, and usage of context information and device policies.


28% 9:36 AM
Work On
Welcome to Work On App
SKIP
NEXT


28% 9:36 AM
Work On
Protected Environment to Work on
SKIP
NEXT


28% 9:36 AM
User Name
Password
LOGIN

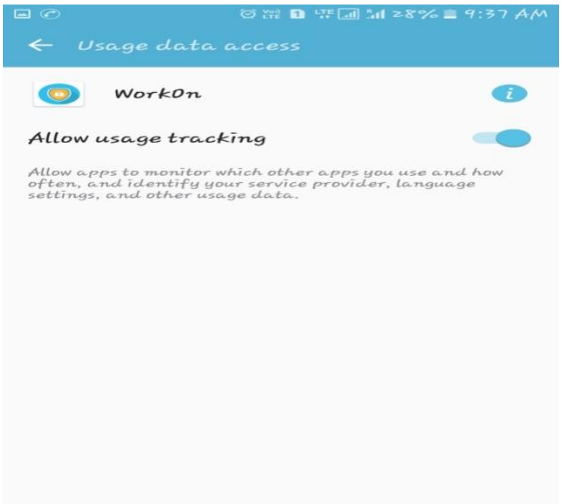


9:36 AM

Logged in Successfully

You have entered safe zone

Some of the apps have been restricted usage here



9:37 AM

Usage data access

WorkOn

Allow usage tracking

Allow apps to monitor which other apps you use and how often, and identify your service provider, language settings, and other usage data.

V. CONCLUSION

Thus we have proposed an application targeted for android mobile and tablet users create a security-aware application that manages access to its content by enforcing device management policies.

When device is protected using this application owner of device decides which content of device will be user see and access it. This application makes changes in OS through application this will help the easy to protect the device from unauthorized user.

REFERENCES

[1] HongLu, “Unobtrusive Gait Verification for Mobile Phones” ISWC '14, SEPTEMBER 13 - 17, 2014, SEATTLE, WA, USA .

[2] Alex Fridman, “DecisionFusionforMulti-ModalActiveAuthentication”,2015

[3] Josef Kittler, “On Combining Classifiers”,IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 20, NO. 3, MARCH 1998.

[4] Ching-Han Chen, “Optimal Fusion of Multimodal Biometric Authentication Using Wavelet Probabilistic Neural Network”, 2013 IEEE 17th International Symposium on Consumer Electronics (ISCE).

[5] Dirk Van Bruggen, “Modifying Smartphone User Locking Behavior”, 2013

[6] Ching-Yi Chen, “Biometric Authentication Using Wavelet Probabilistic Neural Network”, 2013 IEEE 17th International Symposium on Consumer Electronics (ISCE).

[7] Mattias Andersson , Hironao Okada, “Towards Multiple User Active Authentication in Mobile Devices”, IEEE TENCON 2013 Journal Publication.

[8] Dr. Sridhar Mandapati , Sravya Pamidi , Sriharitha Ambati, “Extracting IM evidence of android apps sign in or purchase”, Journal of Computer Engineering 2015.

[9]Abdul Hadi H. Nograles, Felicito S. Caluyo, “Monitoring Temperature Changes in Body”, IEEE INDICON 2013 Journal Publication.

[10] Akshata V.S, Rumana Pathan, Poornima Patil, Farjana Nadaf, “Toward Writing Style Anonymization”, International Journal of Core Engineering and Management(IJCEM) 2014.