VOL. 16, NO. 21, NOVEMBER 2021 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

# A NOVEL APPROACH IN EVALUATING MOBILE USAGE BASED IMPLICIT AUTHENTICATION USING BEHAVIOR CLONING

Md Asifur Rahman and Bodrunnessa Badhon
Department of Computer Science and Engineering, Rajshahi University of Engineering and Technology, Bangladesh
E-Mail: asifurrahman1@gmail.com

**ABSTRACT**

Over the years, mobile device has become the most preferred way to communication, sharing information and even sensitive data. In fact, many security measurements such as 2-step verification, OTP based transaction are also dependent on the authentication of mobile user. A lot of research initiatives have tried to develop both explicit and implicit authentication mechanism for the devices. But implicit authentication measures have gained much attention over the year, as they are more secure continuous measure that can be made undetectable. Majority of the previous studies on implicit authentication of mobile device are mainly focused on analyzing different data attributes in retrieving behavioral traits and using linear techniques to describe an individual's behavioral pattern. On top of that, almost all the previous studies ignores the consideration of analyzing how a user interact with a mobile environment as they are more focused on finding pattern within the retrieved data features. To our knowledge for the first time, this study analyze the user interaction with the mobile phone by mapping them into the Markov Decision Process (MDP) environment and later proposes a RNN agent based technique to extract user's unique policy that could be used as biometric traits. The proposed technique is also able to extract a continually evolving user's policy by incorporating data aggregation while ensuring authenticity. The comparative analysis of the proposed technique clearly indicates the suitability of this approach, as the proposed technique is able to outperform some of the well-known implicit authentication techniques and attain a recognition rate of around 90.38%.

**Keywords:** implicit authentication, behavior cloning, markov decision process, mobile authentication.

## 1. INTRODUCTION

The computational power and storage capacity of mobile phone devices has increase significantly over the years. This has extensively improved the user experience as the user can store a lot of data (public, personal and private) and enjoy superior performance. However, at the same it also brought the concern of device security as exposure of many of these sensitive data can pose great harm to the individuals. As more and more day to day transaction are getting online, it is quite hard to avoid using mobile device and not entering any sensitive data or store sensitive data in device memory or cache. Consequently, authenticating the mobile user has become a crucial task to ensure device security that in turn can also secure the stored data. Majority of the mobile device offers user authentication through alphanumeric passwords, numeric PINs, patterns. However, these techniques are prone to be forgotten or getting stolen and oftentimes users are reluctant to use these measures. As a result, biometric security measures [1-3] have gained much popularity over the years as they can ensure stronger security while providing better user experience. By definition, biometrics refers to unique identification of an individual by using physical or behavioral attributes/traits of that individual. As biometric traits uniquely belong to individuals they do not need to be remembered and are also hard to acquire through stealing.

Considering the significance of biometrics, major mobile manufacturers are now developing mobile device with embedded biometric sensors. Apple introduced the Touch ID technology by incorporating fingerprint scanner, which can be used to lock or unlock the mobile and provide verification before making any purchase. The face unlock feature by Google, uses facial biometric features captured through front camera to perform face recognition and lets the authenticated user to unlock their mobile device. These sensor-oriented biometrics are explicit in nature and requires intentional interaction with the sensors. On the contrary, the concept of implicit identification, which refers to the application of user behavior for authentication, is a very intriguing and more secure means of ensuring authentication. Since implicit identification is more oriented to user's behavioral pattern and habits, it captures the unconscious distinctive pattern of the user behavior and thus it is quite impossible to be replicated by an adversary while at same time this continuous authentication process can be completely invisible. As a result, implicit identification has gained much attention over the years.

In their study, Shi *et al* [4], identified several sensor data such as typing patter, call pattern, voice recordings, calendar entries, accelerometer measurements which can be used to retrieve behavioral pattern. However, retrieving behavioral pattern can be very challenging as majority of the literatures are limited by scalability, large false acceptation and rejection rate [5]. Many study have tried to overcome these limitations and proposes several behavioral biometric traits and recognition techniques [6-9]. In [10], Yazji et al used user's file access pattern and network activity as behavioral biometric traits and proposed a nearest neighbor-based classifier. In a different approach, Premkumar et al. [11] proposed a forest classifier and support vector machine (SVM) based authentication technique that uses data features such as locations, pressure, and touch for authentication. Another remarkable study on behavioral biometric that utilizes user touch, gesture and location as biometric traits is [12]. In this study, Centeno et

al. proposed a Siamese convolutional neural network based OCSVM authentication technique that is capable of attaining a higher accuracy. Meanwhile, El-soud et al proposes a random forest based implicit authentication technique with rank aggregation in [13]. In this study, rather than using user's touch or gesture behavior they consider how a user picks up the mobile device.

Despite all the previous researches, the field of implicit authentication through mobile usage data is still limited by the shortage of large dataset with wide range of continuous data features, lack of scalability of the authentication techniques and lower accuracy with higher false rate of the techniques. Besides, most of the current literature only considers the data feature and ignores one very important fact that every individual acts in a particular way in a particular environment. So it is crucial to incorporate the notion of the environment so that vital relationship among the features and their interaction within the environment could be analyzed. For example, a mobile user might use a particular application with very unique sets of touch and tap gestures. Without considering the whole thing as an environment the observed data would only give us the number of tapping value, finger count during tap, contact size etc. However, by incorporating the notion of environment we can observe the same thing like, while a particular application is open, user tapping action indicates higher touching rates with a greater contact size while the number of finger count being 1. This would allow us to extract more complex dynamics regarding the user mobile usage behavior. With the motivation to further explore this key aspect, this study aims to develop a more dynamic implicit authentication technique. The main contributions of this research are:

- Define a simplified Markov Decision Process (MDP) environment in order to analyze the user's behavioral dynamics related to mobile device usage.
- Apply behavior cloning to retrieve the user's unique policy and later use it as the unique biometric trait for implicit authentication.
- Analyze the recognition rate using the extracted policy based behavioral traits and provide comparative analysis with some well-known techniques.
- To our knowledge, this is the field study to introduce the notion on environment in implicit authentication and analyze user's behavior through state-action pairs.

## 2. PROPOSED METHODOLOGY

In this section, first we are going to discuss our formulated MDP environment for behavioral biometrics and later we are going to discuss our proposed behavior cloning based biometric framework.

### 2.1 Formulated Markov Decision Process (MDP)

In this study we model the MDP environment as a simplified version of Markov Decision Processes (MDPs) [1] that only consists of states s ∈ S and actions a ∈ A. The reward function and corresponding reward from the MDP has been disregarded in our study.

**A) State Representation**

Since this study attempts to apply a user's mobile usage pattern as a unique identification mechanism, the state definition has been formulized considering the data feature that could best identify individual traits and relevancy with standard dataset to validate the proposed approach. In this study, we have used HMOG dataset [14] which is a publicly available database consisting of touch gesture data for reading module, writing module and map module. Therefore, the state of the MDP is also defined in a way to capture the very crucial factors from this dataset such as application usage, gestures etc. Particular information from these factors over time stamps $(t)$ is considered as a state observation $s_t \in S$ for the MDP. A simplified state representation of the MDP is presented in Figure-1.

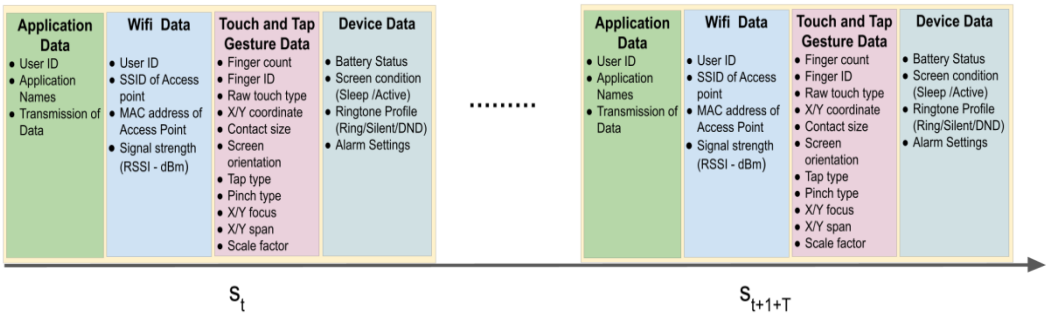


**Figure-1.** State representation of the MDP.

Besides, a mobile phone being idle for a long time or the mobile screen in sleep mode can indicate either a busy time or sleeping behavior of the individual. That is why; in the MDP we are not incorporating any terminating states to capture such events as well.

**B) Action Representation**

The environment of the proposed MDP has a finite set of action which are:

- Open application.
- Close application.

- Turn-on Wifi.
- Turn-off Wifi.
- Raw touch
- Tap gesture
- Scale gesture
- Scroll gesture
- Set alarm
- Change ringtone profile
- Connect to charger
- Disconnect from charger

Since multiple actions can occur at any timestep, in our study we are using an encoded vector to denote the actions at a particular timestep, which is depicted in Figure-2.

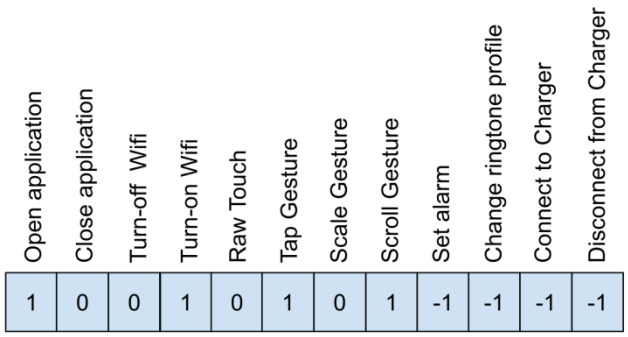


**Figure-2.** Action representation of the MDP.

In the encoded action vector, a zero (0) indicates that no action has been performed, meanwhile a one (1) means that a particular action has been performed while a minus one (-1) indicates to disregard the action. The use of disregard -1 bit is due to the lack of the dataset with these corresponding data features. However, we are proposing the action vector with the disregard bit so it can incorporate any future datasets with these attributes as well.

### 2.2 Proposed Behavior Cloning Based Implicit Authentication

In this study, at the first preprocessing step, we map the dataset to the defined MDP so that we can extract expert demonstration $(D)$ as a tuple of corresponding state and action $(s, a)$ pair and effectively represent them as i.i.d (independent and identically distributed). In the next preprocessing stage, information regarding the applications and tap and touch gestures are encoded to one hot encoding. The other relevant information features are also represented in suitable one hot encoded form and finally all the encoded information are concatenated together so that they can be feed into the corresponding network

In order to reduce compounding error we also use dataset aggregation [15] that incorporates any newly observed states action pair into the expert demonstration, See Figure-4 for more details. The main goal of this study is to retrieve the user's policy that maps the state action pair and use it as the biometric traits for implicit authentication. Therefore, in our approach we are using two agent one is the expert agent and the other one is the biometric agent. The expert agent is constructed of a long short term memory (LSTM)[16] recurrent neural network (RNN) and trained to learn the user's policy, i.e. the function that can predict the next state-action $(s_{t+1}, a_{t+1})$ pair given a current state-action $(s_t, a_t)$ pair as an input from the actual expert demonstration $(D)$. The expert agent and the biometric agent framework are depicted in Figure-3 and Figure-4 respectively.

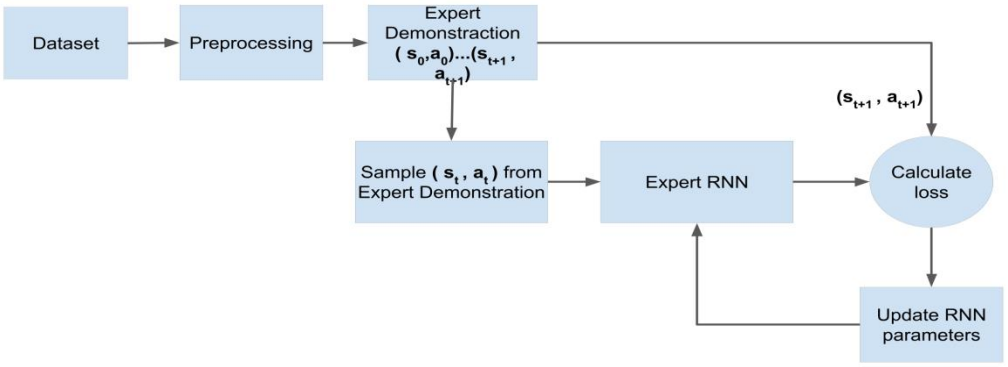


**Figure-3.** Expert agent framework.

On the other hand, the biometric agent possesses the same network architecture as the expert agent and also initialized with the parameters of expert agent's RNN network. In fact, the biometric agent acts like a discriminator that differentiate whether the current user's mobile usage behavior represent by the estimated policy as state-action pair matches with the actual user's policy. Furthermore, the biometric agent is also used to identify and aggregate newly observed state action pair of the actual user. The expert RNN network is retrained after every $W$ timesteps with the newly aggregated expert demonstration, which makes our approach more adaptive to user behavior and less susceptible to compounding error.

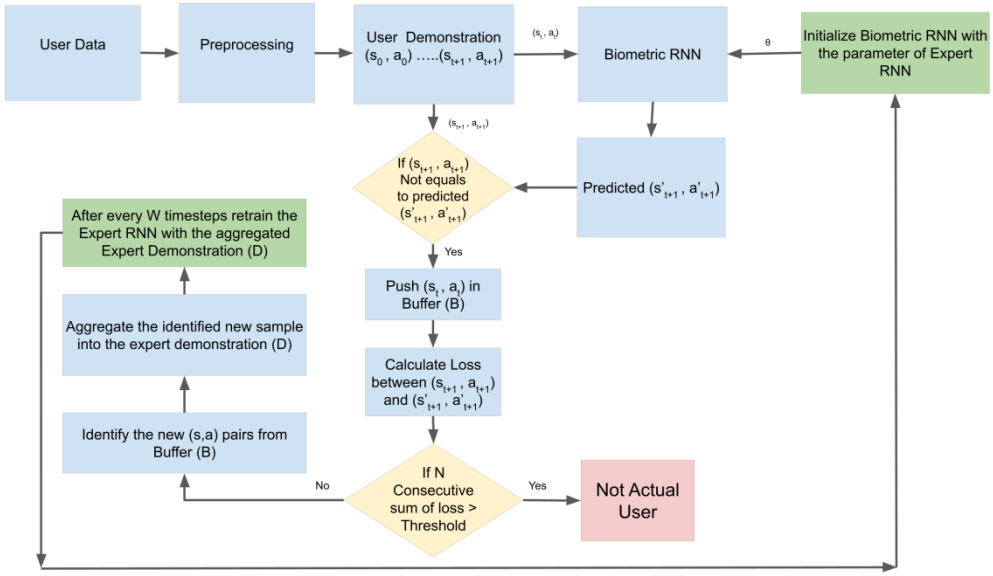


**Figure-4.** Implicit authentication through biometric agent framework.

The encoder and decoder of our expert agent's LSTM network consist of 256 neurons arranged in one single layer. The weights are initialized according to a continuous uniform distribution over the interval of -1 to 1. The learning rate is set to 0.01 with a decay of 70%. We have used the Adam [17] optimization algorithm to update the parameters of the network. We have also set a dropout rate of 40% to avoid over fitting. The embedding layer has 256 neurons that receive a one hot encoded representation of the input. The output layer also contains 256 neurons and the final output is subjected to a post processing steps that transform the network output into corresponding state action pair.

## 3. EXPERIMENTAL ANALYSIS

In this study we have conducted experiment to validate the performance of our proposed behavior-cloning framework and compared it against some of the well-known techniques. For experiment, we have used the publicly available HMOG [15] dataset for the experimental analysis. The overall experimental result has been presented in Table-1.

**Table-1.** Experimental result.

| Method | Recognition Rate | False Positive | False Negative |
|---|---|---|---|
| Yazji et [10] | 82 % | 4.58% | 3.56% |
| OCSVM [12] | 89 % | 4.21% | 3.71% |
| Our Proposed Method | 90.38 % | 2.57% | 1.75% |

From the experimental analysis we can see that our proposed method greatly outperforms the existing technique. The reason for the superior performance can be characterized to several factor. Firstly, unlike the other techniques, in our study we analyze the daily activity of a user and apply them to retrieve the policy function represented by the agent network that can explain user's activity. In other word, we have considered the mobile device as an environment itself and the human as the expert agent that interacts with this environment. This assumption has helps us in extracting important features using behavior cloning which has inevitably increased the performance of our proposed technique. Secondly, the use of LSTM has also help our technique to capture non-linear relationships between the state-action pair as well, which also significantly improves the recognition rate. Finally, by applying the data aggregation method our technique is able to incorporate any newly adopted behavior of the user, which has helped in attaining better recognition accuracy over data features apart by month or weeks.

## 4. CONCLUSIONS

Considering the shortcoming of the previous studies this study adopts a completely new approach in implicit authentication that analyzes the dynamics of mobile user behavior by defining a MDP environment. Unlike the previous studies, majority of which employs device usage data feature as biometric traits, this study extracts the user policy that defines the state-action transition in the MDP and uses it as the biometric traits. Beside retrieval of the user policy using behavior cloning, the proposed method is also able to incorporate new habits or behavioral traits through data aggregation. This enables the learned policy to evolve over time and provide a more accurate implicit authentication. The experimental analysis on standard dataset reveals that the proposed method greatly outperforms the existing well-known techniques. In fact, our environment-oriented analysis of biometric traits

can also be extended to authentication process of other application areas as well. The feature endeavor of this work will focus on reduction of data dimensionality to make the proposed technique more scalable, refining the network architecture or use more complex network architecture, analyze the proposed technique using other large datasets with wide range of attributes.

**REFERENCES**

[1] M. S. Khalil and F. K. Wan. 2012. A review of fingerprint pre-processing using a mobile phone. 2012 International Conference on Wavelet Analysis and Pattern Recognition, pp. 152-157, doi: 10.1109/ICWAPR.2012.6294770.

[2] P. Abeni, M. Baltatu and R. D'Alessandro. 2006. NIS03-4: Implementing Biometrics-Based Authentication for Mobile Devices. IEEE Globecom 2006, pp. 1-5, doi: 10.1109/GLOCOM.2006.276.

[3] R. C. Johnson, W. J. Scheirer and T. E. Boult. 2013. Secure voice based authentication for mobile devices: Vaulted Voice Verification. Defense, Security, and Sensing, doi: 10.1117/12.2015649.

[4] E. Shi, Y. Niu, M. Jakobsson, and R. Chow. 2011. Implicit Authentication through Learning User Behavior. in Information Security, Berlin, Heidelberg. pp. 99-113.

[5] C. Nickel, T. Wirtl and C. Busch. 2012. Authentication of Smartphone Users Based on the Way They Walk Using k-NN Algorithm. 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 16-20, doi: 10.1109/IIH-MSP.2012.11.

[6] W. Meng, D. S. Wong, S. Furnell and J. Zhou. 2015. Surveying the Development of Biometric User Authentication on Mobile Phones. in IEEE Communications Surveys & Tutorials, 17(3): 1268-1293, thirdquarter doi: 10.1109/COMST.2014.2386915.

[7] H. Ketabdar, M. Roshandel and D. Skripko. 2011. Towards implicit enhancement of security and user authentication in mobile devices based on movement and audio analysis. In ACHI 2011, The Fourth International Conference on Advances in Computer-Human Interactions. pp. 188-191.

[8] M. Jakobsson, E. Shi, P. Golle and R. Chow. 2009. Implicit authentication for mobile devices. In Proceedings of the 4th USENIX conference on Hot topics in security (HotSec'09), pp. 9-9. USENIX Association.

[9] N. A. Safa, R. Safavi-Naini and S. F. Shahandashti. 2014. Privacy-Preserving Implicit Authentication. in ICT Systems Security and Privacy Protection, Berlin, Heidelberg. pp. 471-484.

[10] S. Yazji, X. Chen, R. P. Dick and P. Scheuermann. 2009. Implicit User Re-authentication for Mobile Devices. In Ubiquitous Intelligence and Computing, pp. 325-339. Springer 2009. doi:10.1007/978-3-642-02830-4_25.

[11] S. Premkumar, C. Samuel, H. P. C. Duen, Z. Hongyuan, Latentgesture. 2014. Active user authentication through background touch analysis. In Proceedings of the Second International Symposium of Chinese CHI., New York, NY, USA, ACM, pp. 110–113. doi:10.1145/2592235.2592252.

[12] M. P. Centeno, Y. Guan and A. van Moorsel. 2018. Mobile based continuous authentication using deep features. in Proceedings of the 2nd International Workshop on Embedded and Mobile Deep Learning. pp. 19-24.

[13] M. W. Abo El-Soud, T. Gaber, F. AlFayez and M. M. Eltoukhy. 2021. Implicit authentication method for smartphone users based on rank aggregation and random forest. Alexandria Engineering Journal, 60(1): 273-283, doi: 10.1016/j.aej.2020.08.006.

[14] Z. Sitová et al. 2016. HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users. in IEEE Transactions on Information Forensics and Security, 11(5): 877-892, doi: 10.1109/TIFS.2015.2506542.

[15] S. Ross, G. Gordon and D. Bagnell. 201. A Reduction of Imitation Learning and Structured Prediction to No-Regret Online Learning. in Proceedings of the Fourteenth International Conference on Artificial Intelligence and Statistics, 15: 627-635. [Online]. Available: https://proceedings.mlr.press/v15/ross11a.html

[16] S. Hochreiter and J. Schmidhuber. 1997. Long Short-term Memory. Neural computation, 9: 1735-80, doi: 10.1162/neco.1997.9.8.1735.

[17] D. P. Kingma and J. Ba. 2014. Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980.