# Continuous User Authentication with Continuous Learning

Suman Kumar
*M.Tech (CSE)*
*IIIT Delhi*
New Delhi, India
suman17060@iiitd.ac.in

***Abstract*—In todays life, computing devices such as smartphone, PC, tablets, and smartphones become an integral part of our life. Its importance can be seen from the facts that todays smartphone contains every documents and sensitive data. But as the smartphone can be stolen easily and in such a situation it's easy for attackers to access the confidential data. Also, the current one-time authentication system provides one-time authentication at login time. Also, there is a restriction on the length of the password on the smartphone which makes authentication more vulnerable on the smartphone. So there is a need for continuous authentication which continuously authenticates the user without interrupting the user and also continuously learning the user changing behaviour.**

***Index Terms*—continuous user authentication, MDP, value iteration, policy iteration, smart devices**

## I. Introduction

Smart devices pose limited authentication approaches such as one-time authentication using pattern, fingerprint and face recognition. Also due to size constraint, passwords length is shorter. And if these one-time authentication breaches, then all sensitive data can be easily leaked and misused. Also, smart devices can be easily stolen and lost which poses a severe risk to the people.

One approach is by installing a central server which continuously authenticates the user. But this requires extra hardware i.e. central server and if this central server caught by the imposter, then all persons sensitive data can be stolen and misused. In these days, continuous authentication is also becoming very popular because of the security requirement in these places is very important.

In this paper, applied the continuous authentication mechanism which continuously authenticates the user which is unnoticeable to the user. So the whole user session is continuously authenticated and continuously learning happens. So we applied the technique Markov decision process(MDP) which continuously authenticate the user session along with continuous learning. So in this approach, smartphone screen divided into cells and each cell tries to capture the user behavior. So if a particular cell is heavily used by the user, then its reward value will be high. So here user behavior is captured as finger movement happen from one cell to another and these ways a particular user movement is captured. The advantage of this approach is the continuous learning, so as the user behavior changes as the time progresses, then our technique will adapt to this new change. Also, our authentication mechanism is better than other approaches as user remain unaware of this authentication mechanism and gives higher accuracy.

The organization of this paper is as follows: section II talks about Related Work. Section III discusses the technique applied in this paper. Section IV talks about the our approach and how we implement policy iteration and value iteration in our project. Section V talk about the conclusion and result. And finally Section VI display the references.

## II. Related Work

In this section, we will briefly discuss about the recent techniques which is used for the continuous authentication. In recent past, along with using swipe gesture for smart devices for continuous authentication, mouse movement and keystroke pattern has also used in recent past for continuous authentication.

Everitt and McOwan [1] were the first to investigate the usage of mouse operating style for continuous authentication in 2003. The research on continuous authentication was started by Shepherd [2] in 1995 and showed the impressive result using keystroke pattern of users. Nui and Hao [3] implemented the continuous authentication using user behavioral features in a multi-touch environment. Their experiment shows the equal error rate of 7% to 15% for one mode. Frank, et al., [4] also conducted the continuous authentication using touch gesture having EER of 4% using k-Nearest Neighbor and Support vector machine classifier. All the above experiment consists of one-time authentication and then continuous learning. It doesnt incur learning during authentication. While using above technique for user authentication, and If user behaviour changes happen, then the whole re-training needs to be done.

So to avoid such a scenario of re-training on every user behaviour change, MDP approach is applied in this paper which continuously authenticate the user while continuously update the user changing behavior. Another advantage is that there is no requirement for extra hardware. Also, user who is using this system remain unaware of his continuous authentication.

## III. Methods

Our project is based on MDP to authenticate the user while continuous learning continuously. Furthermore, applied the policy iteration and value iteration for policy and value function update.

### A. MDP

In reinforcement learning problem, the task of the agent is to interact with the environment. At each time step, the agent acts in a particular state: it reaches to a new state and receives the reward. The goal of the agent is to learn optimal policy which maximizes the total reward received by the agent. The reinforcement learning task that follows the Markov property is called the Markov Decision Process(MDP). If the state and action in the MDP are finite, then it is called finite markov decision process. A finite MDP is particular important as it follows one step dynamic of the environment. So MDP is defined by five tuple (S, A, P, R, $\gamma$) where

- S is the set of states
- A is the set of actions
- P is the transition probability

$$P_a(s, s') = P_r(s_{s+1} = s'|s_t = s, a_t = a)$$

- R is the rewards
- $\gamma$ is the discount factor which control the future rewards

### B. Value Iteration

Value iteration calculates the optimal state value function by continuously estimating the V(s). Initially, V(s) is initialized with a random value. It continuously updates the Q(s, a) and V(s) until converges. It guarantees to converge to the optimal value.

Below is the pseudo-code for value iteration.

- Initialize each state with random value
- For each state, calculate the new V, based on its surrounding state
- Update the each state V based on above calculation

$$V_{i+1}(s) = R(s) + \gamma max_a \sum_{s'} T(s, a, s')V_i(s')$$

- if No value change by delta value, then halt

### C. Policy Iteration

Value iteration keeps on improving value function at each iteration until the value function converges. But policy iteration rather than improving value function at each iteration, it defines policy at each step and computes value according to this new policy until converges. Policy iteration too converges to optimal policy and policy iteration take less iteration than value iteration to converge. Also, policy iteration has some prior knowledge of the plans, so it converges faster.

Below is the pseudo-code for policy iteration.

- Initialize random policy for each state
- Repeat the following
- initially $\Pi$ = $\Pi$ '
- compute the value using $\Pi$ by below equation

$$V^{\Pi}(s) = R(s) + \gamma \sum_{s' \in s} P(s'|s, \Pi(s))V^{\Pi}(s')$$

- Improve the policy at each state

$$\Pi'(s) = argmax_a(R(s) + \gamma \sum_{s' \in s} P(s'|s, a)V^{\Pi}(s'))$$

- until $\Pi$ = $\Pi$ '

## IV. Dataset Description

In this project, HMOG [5] (Hand Movement, Orientation, and Grasp) dataset is used which contains behavioral features to authenticate the smart phone users continuously. HMOG uses magnetometer, gyroscope and accelerometer for capturing micro hand movement and orientation pattern when user tap on the smart phone screen. Data collected from three usage scenarios such as document reading, text writing and navigation on map. A total of 100 volunteers contributed for data collection. Each volunteers perform random work assign to them. For each volunteer, 24 different session made and data collected in that session. Each user data collected around 2 to 6 hours. Each session collected data for categories such as accelerometer, gyroscope, magnetometer, tag gesture, row touch count, scale gesture, key press, etc. The total size of the dataset is 6 GB. The dataset collected under two conditions such as sitting and walking.

## V. Approach

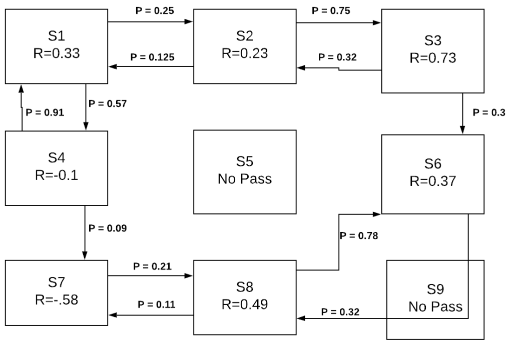

Fig. 1. MDP approach on smartphone cell

Initially, we divided the touch screen into the 8*6 grid. So we have a total of 48 states which correspond to the number of states in MDP. The possible action from one state is going from that state to all other states. In our experiment, we have consider only two actions: 0 corresponds to remain in the same state and 1 corresponds to moving to some other state. Also, transition probability and reward value initialize to a very small value(0.0001). Also, policy and value function corresponding to each state is initialize to random value in beginning.

Initially, dataset collected in millisecond. So directly working with milliseconds data doesnt capture any movement. So

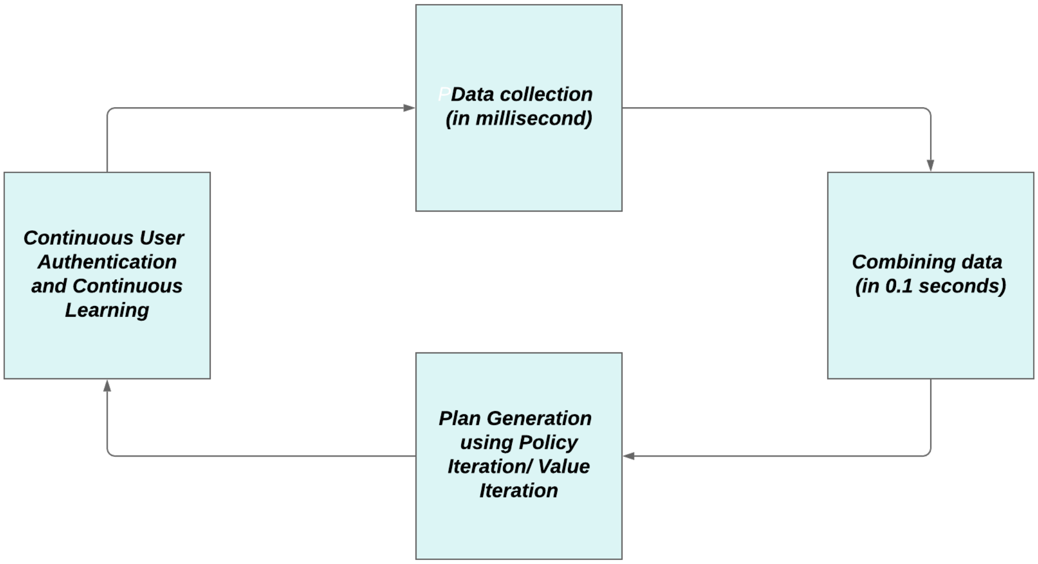

Fig. 2. Methodology

we combined the data for every one tenth of seconds and then applied the value iteration and policy iteration. Each user consists of 24 distinct session. So the first twenty sessions are used for training and the last four sessions used for testing.

During the training phase, the user performs a sequence of actions and corresponding transition probability and reward matrix of the respective state gets updated. And after, every one-second interval, policy iteration, and value iteration is performed and the corresponding policy and value function of each state is modified. Finally, after training on twenty sessions, policy and value function is obtained.

During the testing phase, we performed the continuous authentication by matching action performed by the user to the actual policy of that state and accuracy is calculated. And continuous learning is performed by performing policy iteration and value iteration after one minute time interval. So this way continuous authentication and continuous learning is performed in testing phase.

## VI. Result and Conclusion

The authentication is checked in the testing phase after every 30 seconds. For the duration of each 30 seconds, the user chosen action matched with the actual policy of that state. So for accuracy calculation, actual matched count is divided by total action taken in these 30 seconds. Here, the reward metrics used as

$$Reward = 1 + alpha * pressure$$

$$where, 0 < alpha < 1.$$

So for four users, we have plotted the accuracy graph vs different session. The average accuracy remains around 50% to 60%. Another reward function chosen as distance + pressure, but accuracy remains around the 50% to 60%.

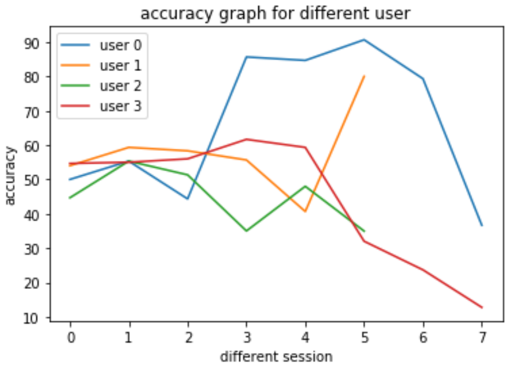

Fig. 3. Accuracy graph for different user

In this paper, we implemented the MDP based continuous authentication approach with continuous learning. The advantage of this approach is that it doesnt require any extra hardware. Also, it doesnt enforce any extra work on the user, and the user remains unaware of this authentication. But our accuracy is very low. This may because reward function needs to be more accurate which enforce the policy iteration and value iteration to capture the correct user movement. Also, the grid size of the screen needs to be more smaller. Till now, only consider the touch event data, but can also use the accelerometer, gyroscope and magnetometer data to capture the user authentication better.

## Acknowledgment

I would like to express my deepest gratitude to my teacher and advisor Dr. Arun Balaji Buduru for his constant guidance and support. This project would not have been possible without his guidance. Special thanks to Rakesh Singh Rawat for constant discussion throughout this project. Also, Special thanks to Vaibhav Garg for keeping me motivated.

Lastly, I like to thank my family member and friends who always motivated and encouraged me.

## REFERENCES

[1] R. Everitt and P. W. McOwan. Java-Based Internet Biometric Authentication System. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003, 25(9): 1166-1172.

[2] S.J. Shepherd. Continuous authentication by analysis of keyboard typing characteristics. In European Convention on Security and Detection, pages 111114, 1995.

[3] Y. Niu, and C. Hao ”Gesture authentication with touch input for mobile devices.” Security and Privacy in Mobile Information and Communication Systems, Springer, Berlin Heidelberg, 2012, pp. 13-24.

[4] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, ”Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication.”, IEEE Trans. Information Forensics and Security, (2013), Vol: 8(1), pp. 136-148.

[5] Zdeka Sitov, Jaroslav ednka, Qing Yang, Ge Peng, Gang Zhou, Paolo Gasti, Kiran S. Balagani. HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users. In IEEE Transactions on Information Forensics and Security, vol.PP, no.99, pp.1-1.