ENHANCED MOVING TARGET DEFENSE MECHANISMS TO HANDLE CYBER ATTACKS

CHAPTER 6

Robust Cryptographic Authentication using Mouse Dynamics

In order to handle the unknown cyber attacks, four moving target defense mechanisms are enhanced in this research work. The chosen four moving target defense mechanisms are

i. **Smart Motion Adaptation/Management – Game Theory**
ii. **Robust Cryptographic Authentication – Mouse Dynamics**
iii. **Data Chunking and Decentralization**
iv. **Decoys**

Robust cryptographic authentication - Mouse dynamics based approach is discussed in this chapter. The enhancement of the existing work is done by integrating manhattan distance and dynamic time wrapping with anytime algorithm for more accuracy in measuring the distance and to reduce the computational time.

6.1. Proposed Research Work using Enhanced Mouse Dynamics

The overview of the proposed work focuses on enhanced mouse dynamics[4] for biometric authentication. The primary goal of this enhanced mouse dynamics research work is to develop to a security mechanism for protecting the information and to ensure user authentication [32]. In order to calculate the distance of mouse operations, integrated graphical password, Manhattan distance with dynamic time wrapping are used. To enhance its efficiency and to increase the accuracy, the existing method is integrated with anytime algorithm[27][73]. The proposed method consists of four steps. They are discussed in the following section.

6.2. Phases of the Research Work

The flow diagram of the enhanced mouse dynamics, the processing steps and proposed algorithm are discussed in this section:

6.2.1. Flow diagram of the proposed method

The flow diagram of the proposed method is given in figure 6.1.

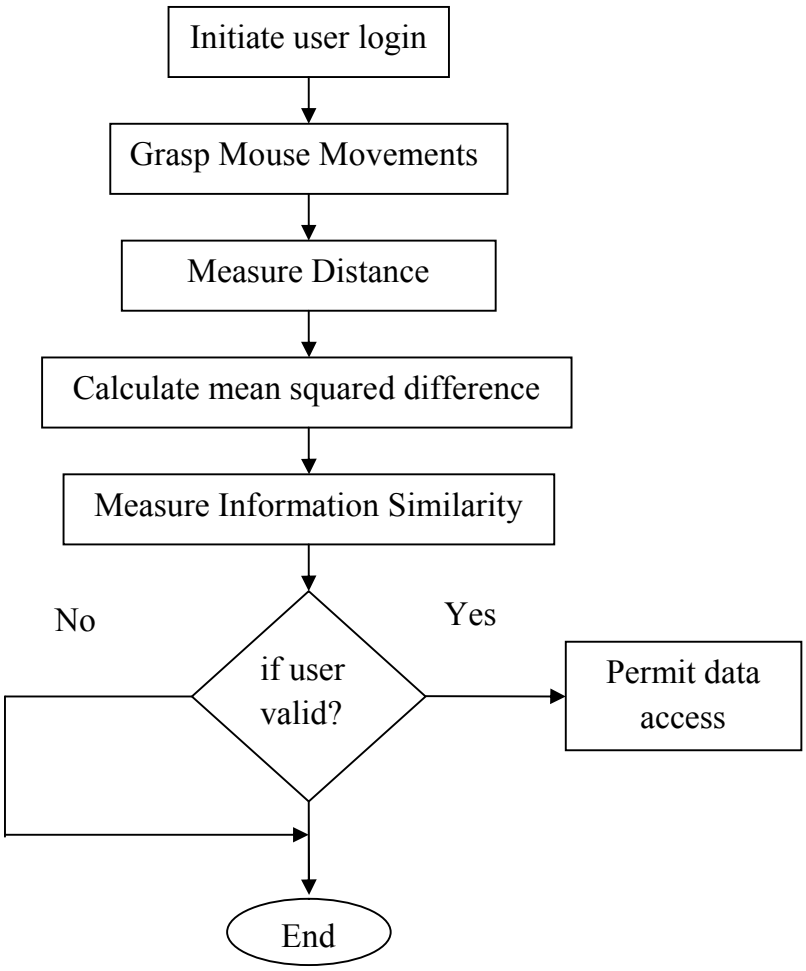

Figure.6.1 Flow diagram of the proposed method

6.2.2.Main Steps of Enhanced Mouse Dynamics

The four processing steps involved of the proposed method is discussed below

Step.1 Initiate user login using graphical password

The users are expected to execute the graphical password to login to access the data base.

Step.2 calculate distance measurements of capturing mouse operation

The mouse operation of every user is measured using integrated Manhattan distance with dynamic time wrapping.

Manhattan distance[31] (MD) calculates the sum of difference in every dimension of each vector. It is otherwise known as L_1 distance. If u=(x_1, x_2,...x_n) and v=(y_1, y_2,... y_n)are two vectors in n dimension. Then MD (u,v) will be calculated using the following equation.

$$\text{MD}(u,v) = |x_1 - y_1| + |x_2 - y_2| + \ldots\ldots + |x_n - y_n|$$

$$= \sum_{i=1}^{n} |X_i - Y_i|$$

Step.3 Measure operations similarity based on anytime algorithm

The similarity of the mouse operation of every user is compared by calculating mean squared difference.

Anytime algorithm is used to measure similarity of the mouse operations, that can be achieved using function as $D(\varphi)$, $D(\varphi,p)$ as parameters and p as percentage of pixels. Mean square difference is measured using the following equation:

$$D_{MSD}(\varphi,p) = -\frac{1}{\lfloor pN \rfloor} \sum_{i=1}^{\lfloor pN \rfloor} \left(R(x_i) - T(W(x_i,\varphi))\right)^2$$

D_{MSD} -Average of the negative mean squared differences in intensity between pixels

N - total number of pixels

p - percentage of pixels

R - Random Order

D – Measure the similarity between a fixed reference image

W(x,) – warped coordinate space

T(W(x,)- new image

Step.4 Authenticate user and permit data access

After executing the anytime algorithm for user authentication, the authorized users will be permitted to access the data.

The main idea of this research work is to enhance the mouse dynamics. The existing method is integrated with anytime algorithm. This integration helps to ensure user authentication in minimum time and increases accuracy in detection of cyber attacks. The same procedure will be executed for every user.

6.2.3. Algorithmic Steps of the proposed research work

The proposed algorithm is given below in table.6.1:

Table.6.1 Proposed Algorithm

```
Initialize server
 for each user logging in
    execute graphical password
     capture mouse operation
      distance measurement
      measure similarity using mean squared difference using anytime algorithm
    ensure user authentication
 if user authorized
 permit to access data
 end if
end
```

6.3 Performance Metrics

The performance metrics used to evaluate the proposed method are:

False Acceptance Rate

The false acceptance rate is a fraction of negative entry or unauthorized user was incorrectly identified as positive entry or authorized user and it will be calculated using the following formula:

$$FAR = \frac{number\ of\ \ false\ accep\tan ces}{number\ of\ client\ accessses}$$

False Rejection Rate

The false rejection rate is a fraction of positive entry or authorized user that was correctly identified as negative entry or unauthorized user and it will be calculated using the following formula:

$$FRR = \frac{number\ of\ \ false\ rejections}{number\ of\ client\ accesses}$$

6.4. Results and Discussions

The experimentation is conducted randomly for 100 participants it covers age group from 20 - 60. The training and testing are given to the proposed method. 100 user's mouse operations are trained and stored in database and the results are obtained for every 25 users.

Table.6.2 Comparative Results of FAR, FRR and Authentication time

No. of Mouse operations	False Acceptance Rate (%)		False Rejection Rate (%)		Authentication Time (seconds)	
	Mouse Dynamics	Enhanced Mouse Dynamics	Mouse Dynamics	Enhanced Mouse Dynamics	Mouse Dynamics	Enhanced Mouse Dynamics
25	5.7	**4.6**	4.3	**3.6**	9.0	**8.7**
50	6.7	**5.8**	4.7	**3.8**	8.9	**8.6**
75	7.7	**6.4**	5.7	**4.6**	8.9	**8.4**
100	8.2	**6.5**	6.7	**5.2**	8.7	**8.1**

Table.6.3 Attack Detection Rate

Attack Types	Mouse Dynamics	Enhanced Mouse Dynamics	Percentage of Improvement
Active Attacks	68%	71.5%	**3.5%**
Passive Attacks	71%	73%	**2%**

6.5. Chapter Summary

The method proposed here enhances the click dynamics for user authentication. The concepts of Graphical Password, One class classifier, Manhattan distance with Dynamic Time Wrapping and Anytime Algorithm is used to increase the accuracy in user authentication. The accomplishment of the proposed method is evaluated in terms of performance metrics like false acceptance rate, false rejection rate, authentication time and attack detection rate to predict its efficiency in defending against cyber attacks. The enhanced mouse dynamics perform better than the enhanced game theory in detecting the cyber attacks. The detection rate is increased to 2% than the enhanced game theory. In the next chapter, improved data chunking is implemented.