Singaporean Journal of Scientific Research

IJCN Special Issue - Data Management and Network Control in Wireless Networks (SICN)
Singaporean Journal of Scientific Research(SJSR)
Vol 6.No.32014 Pp.186-193
Available at:www.iaaet.org/sjsr
Paper Received:14-03-2014
Paper Accepted:29-03-2014
Paper Reviewed by:1Prof.Dr.Ponnambalam 2. Chai Cheng Yue
Editor: Dr. Binod Kumar

DYNAMIC AUTHENTICATION BASED ON ACCELEROMETER DATA IN WIRELESS SENSOR NETWORKS

M.Sivaraja[1] J.Kokila[2]
[1,2]Dept. Of CSE,
[1]*K.Ramakrishnan College ofTechnology*
[2]National Institute of Technology
Trichy, Tamilnadu
Email: sivaraja96@gmail.comjk.cse09@gmail.com

ABSTRACT

Access control is a mechanism which enables an authority to control access to restricted areas and resources at a given physical facility or computer-based information system. To the static identification information exchange among the access cards and access control clients, it is very challenging to fight against access control system breaches due to reasons such as loss, stolen or unauthorized duplications of the access cards. Although advanced biometric authentication methods such as fingerprint, face recognition and iris identification can further identify the user who is requesting authorization. To introduce a dynamic authentication with sensory information for the access control systems. They are able to significantly increase the security key space *P* and hence the level of security for existing electronic authentication systems. A wide variety of sensors including accelerometer, gyroscope and etc. can be used in this system. To illustrate the basic concept and the resulting security enhancement of this sensory data and service provider data to controlled the enhanced access control system design, to use accelerometer sensor. The sensory data generated from the rotation of accelerometer to introduce a reference design for the proposed sensory data enhanced authentication scheme. Simple rotations can increase by more than 1, 000, 000 times with an authentication accuracy of 90%. The service provider data generated by the service provider system to send by the users mobile number on running time. By combining the both keys are verified and validated to allowed the process. To performed extensive simulations under various environment settings and implemented the design experimentally verify the system performance.

Index Terms— Authentication; Sensory Data; Access Control System; Wireless rechargeable sensor.

1. INTRODUCTION

Access control is the selective restriction of access to a place or other resource. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authentication. In general, authentication methods in access control systems can be divided into two broad categories. The first category is based on mechanical matching, such as keys and combination locks. Individuals are authenticated in these access control systems if and only if the blade of the key matches the keyway of the lock or the correct numerical sequence for combination lock has been dialled. Due to the physical constraints of mechanical matching systems, they are insufficient to meet the demanding requirements of access control authentication for critical infrastructures.

The other category of authentication for access control systems is electronic authentication including barcode, magnetic stripe, biometrics and etc. However, it still suffers from similar problem of key loss since authentication is only based on the encoded identification data on the card. In this work, we aim at bridging the gap between insufficiency of existing electronic authentication solutions and the increasing demand of high security guarantee for access control systems. We design a novel electronic proximity authentication framework that enhances the security level of existing RFID-based access control systems[1], [4] with backward compatibility. our contributions in this work are as follows:

- We design and implement a dynamic authentication framework with sensory information for the access control systems. Our design is backward compatible with existing, deployed RFID or access card readers.
- We have full implemented and built a running prototype of the proposed dynamic authentication frame-work on the Intel Wireless Identification and Sensing Platform (WISP). Based on the running prototype, we have extensively evaluated our design in terms of system accuracy and usability in the real-world settings.

2 RELATED WORK

The existing electronic proximity authentication of access control systems is mainly based on the exchange of encoded identification information stored on the access card. The security and integrity of such static and passive authentication mechanisms suffer from problems such as access card loss and unauthorized duplications. To propose to use sensory information obtained from wireless rechargeable sensors on access cards to further enhance the security and robustness of existing electronic proximity authentication systems. The main idea of system design is show in Figure 1. when an access card integrated with wireless rechargeable sensors enters the communication range of an access control client; the access card piggybacks its sensory data to conventional identification information and transmits it (i.e. the electronic key) to the access control client. The information received by the access control client is then forwarded to the network server for authentication. If both sensory data and identification match a valid record in the authentication database, the network server then instruments the actuator and grants the card holder the access to the system. In this way, even an authentic access card is in possession of a unauthorized personnel or has been illegally duplicated, as long as the unauthorized card holder does not know how to generate the correct sensory data, he or she still cannot access the system. Moreover, to successfully remove the system vulnerable period between loss/stolen of access card and the deactivation of the card after users' report.

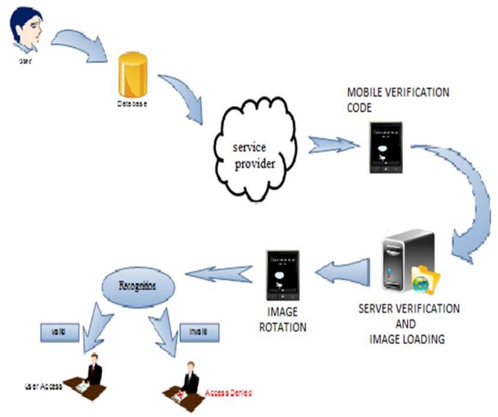


Figure. 1. System Function Diagram

On the contrary, trusted users can share the cards and predefined actions with each other which is unavailable in biometric authentication systems. Different from existing authentication methods such as combining RFID and an additional keypad near the reader, to propose an orthogonal design and the new authentication framework only revises authentication algorithm on the network server without any modification of access clients. In fact, since piggyback sensory data to ID information before transmitting them to the reader, most existing works on communication encryption for RFID system can be easily adopted into authentication method and therefore deal with several security vulnerabilities such as replay attack and eavesdropping. The identification information on access cards normally is static. The user swipe a access card to send a request to the service provider system. In service provider make a authentication code to send the user mobile. When the user enter the code to verified by the server side database. If the data's are correct to load the images to make the rotation process. User's make the rotation's on the image to generated the electronic key. The electronic key is verify the database. If the electronic key is correct to allowed the user to the process. User make a wrong rotation's not allow the process. we propose an orthogonal design in this paper and the new authentication framework only revises authentication algorithm on the network server without any modification of access clients.

With the addition of dynamic sensory data from on-board sensors, they are able to significantly increase the security key space *P* and hence the level of security for existing electronic authentication systems. A wide variety of sensors including accelerometer, gyroscope and etc. can be used in system. In particular, to utilize the sensory data generated from the rotation of accelerometer and gyroscope to introduce a reference design for the proposed sensory data enhanced authentication scheme. Through prototyping system and real world experiments, to demonstrate such a rotation-based design is a feasible and practical option for the proposed generic dynamic authentication framework.

*A.Accelerometer-based Reference Design:*For an accelerometer, if it is being rotated, the static acceleration of gravity on its three axes will change accordingly [2]. For a two-dimensional rotation, we can calculate the tilt angle *α* of an accelerometer from static acceleration of gravity on its X-Axis and Y-Axis to determine the position of the accelerometer in a two-dimensional plane.

- Basic rotation parameters:
  - **Granularity of the Rotation Recognition n:** Every two different positions with their tilt degree gap bigger than (2*π/n*) can be identified and *n* refers to the maximal number of recognizable rotations within one round.
  - **The Number of Basic Rotations k:** The number of basic actions performed in one rotation sequence.

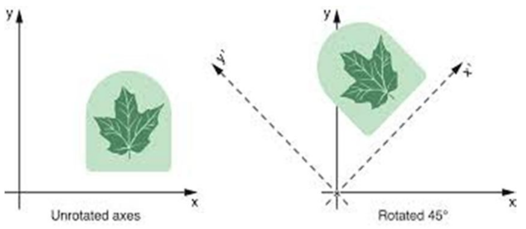


Figure. 2. Rotation Sequence Diagram (2D)

Figure 2, shows an example of rotation sequence with three basic rotations (*k* = 3) and granularity of the recognition *n* = 8. CW respectively. In Figure 3, initially the accelerometer is tilted ${}^{\pi}/_{4}$ degree to the Y-Axis. Then the accelerometer is rotated ${}^{\pi}/_{2}$ degree clockwise, ${}^{3\pi}/_{2}$ degrees counterclockwise and degrees clockwise, respectively. We can represent the multitude of the key space increase for a two-dimensional rotation by the following equation:

$$P_{acc}^{2D}(n, k) = n[2(n-1)](1)$$

In Equation 1, *n* denotes the number of different possible starting positions for the first basic rotation. Then for the following *k* rotations, we just need to determine the direction, we can either clockwise or counterclockwise rotate the accelerometer to all other *n*−1 possible positions [3].

B.Three-Dimensional Rotation: In this part, we extend our design to rotations in three- space. Since determining the attitude of sensor solely dimensional based upon static acceleration of gravity is impossible. Based on the relative positions of the accelerometer and the ground, we extend the basic two-dimensional rotation rules for three-dimensional rotations: (i) During the whole rotation process either plane *XY* , *Y Z* or *XZ* under the coordinate of accelerometer is perpendicular to the ground (ii) Accelerometer only rotates in one plane under its own coordinate (*XY* , *XZ* or *Y Z*) during one basic rotation;

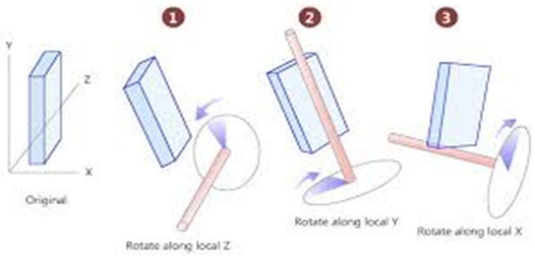


Figure. 3. Rotation Sequence Diagram (3D)

In Figure 3, each action between two consecutive positions is a plane rotation, and rotation plane could changes only when the direction of static acceleration of gravity is consistent with the direction of axes in accelerometer's coordinate [3].

On the basis of the rules above, the starting position of each basic rotation can be divided into two types on whether one of axis ±*X*, ±*Y* and ±*Z* is perpendicular to the ground at the beginning of the basic rotation. According to the third rule, if one of the axes is consistent with the direction of gravity, the following action can occur in two different planes. However in the other case, the following basic rotation can only generated within a fixed plane.

$$P_{acc}^{3D}(n, k) = a_{k+1} + b_{k+1}$$

where

$$a_{k+1} = 2 \cdot 2 \cdot 3 \cdot a_k + 2 \cdot 4 \cdot b_k$$

$$b_{k+1} = 2 \cdot 2 \cdot (n-4) \cdot a_k + 2 \cdot (n-5) \cdot b_k$$

$$n = 4m,\ m \geq 1 \in N$$

value $a_0 = 6$ and $b_0 = 3(n-4)$, $n = 4m$, $m \geq 1 \in N$.(2)

Recursive formulae of both a_k and b_k in Equation 2, consist of two parts that calculate key spaces under different initial positions of the accelerometer. For example for a_k,2 · 2 · 3mean two feasible directions, two feasibleplanes and three feasible end positions of one basic rotation respectively.

C.Gyroscope-based Reference Design: Gyroscope is a device for measuring change of orientation.

Therefore it is also possible to utilize the action of rotation of a gyroscope in a three-dimensional space since it re-turns the angular velocity on each axis simultaneous when rotating. Imaging there is a ball with centre, Figure 4 depicts six standard rotations of the ball using vectors. Corresponding sensory data of the six basic rotations of a typical three-axis gyroscope.

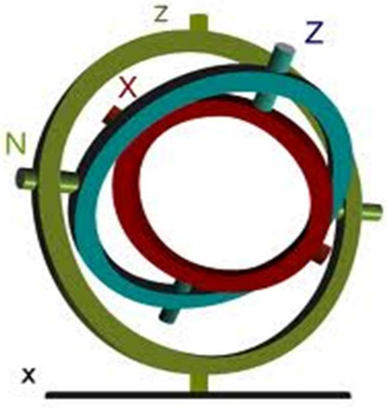


Figure. 4. Standard Rotations of a Gyroscope

3 PROPOSED DESIGN

Different from accelerometer-based design which relies on precise rotations, higher rotation speed of the gyroscope leads to a higher output value which make it easier for authentication. In this gyroscope-based reference design, we only use such binary rotation information (whether rotated) at each axis to perform sensory-data based authentication. Therefore, the key space increase can be written as

$$P_{gyro}(k) = [3 \cdot 2 + ({}_{3}^{2}) \cdot 2 \cdot 2]^{k} = 18^{k} (3)$$

The base of Equation 3, consists of two parts that compute the composition of feasible rotation directions of one basic rotation. Since the gyroscope has three axes and it can rotate on each axis with two directions, there are $3 \cdot 2$ feasible rotation directions if the gyroscope rotates on one axis. If values on two axes change during a basic rotation, the total feasible rotation directions can be written as $({}^{2}{}_{3}) \cdot 2 \cdot 2$.

3.1 Rotation Identification

In the previous section, we discuss the potential of large key space increase for our dynamic authentication with sensory information design. Dynamic authentication with sensory information design. Further elaborate on the detailed sensor rotation recognition algorithms. By comparing the sample data of accelerometer. To find that output of the accelerometer exhibits a more complex behaviour. This is because gyroscope measures the angular velocity and tends to generate an impulse during one single basic rotation, which could be treated as a special case of the output of the accelerometer.

Therefore to use the sensory data of accelerometer to illustrate the whole rotation recognition algorithms and discuss how to deal with the sensory data of gyroscope. One complete dynamic authentication process consists of a sequence of basic rotations. In order to accurately identify each individual basic rotation from raw accelerometer data, to perform following three operations in the network server.

A. Data Pre-Processing: The first step of rotation recognition is data pre-processing. The main goals are to separate and filter each individual basic rotation from a series of raw accelerometer data. In order to separate the individual basic rotations, first need to identify the pause between two consecutive rotations. During such pauses, the three-axis readings of an accelerometer would remain relatively stable and unchanged for a short period of time.

Recognize such pauses and separate different basic rotations, to adopt a slidingwindowapproach. The accelerometer readings in the first *tw* second are buffered into the sliding window. All data in the sliding window are then fitted by a first-order polynomial function. If the coefficient of first-order polynomial is less than a threshold (1 in our implementation), to consider the accelerometer remain stationary within the time frame of this window. Followed by this pause detection in the current window, the window would slide for a step of *ts* seconds, with *ts* duration of new data appended to the end of the sliding window while the first *ts* duration of sensory data are discarded. Empirically, set *tw* = 1*s* and *ts* = 0.3*s* in system implementation. In this way, it achieved accurate separation of basic rotations in one complete authentication. To visualize above data pre-processing step, one authentication with 4 basic rotations that performed slowly on prototype implementation. The shaded regions represent sliding windows at three pauses, it can be found that the accelerations on three axes of the accelerometer are rather stable during pauses between different basic rotations.After identifying pauses between basic rotations, then use least square estimation to fit the raw readings for each individual basic rotation from the accelerometer.

Assuming the accelerometer readings for basic rotation on one of the three axes is:

$p_i = (x_i, y_i), i = 0, 1, 2, \cdot \cdot \cdot , m$

Then the least square estimation tries to build a polynomial function below:

$$y = f(x) = a_0x^m + a_1x^{m-1} + \cdot\cdot\cdot + a_{m-1}x + b$$

such that

$$\min(F(a_k, b)) = \min(\ \textstyle\sum (f(x_i) - p_i)^2)$$

$$= \min(\ \textstyle\sum (f(x_i) - p_i)\ )(4)$$

$$k = 0, . . . , m - 1$$

we discuss fitting effect in detail and make the decision of *m* through prototype experiments.

B. Feature Vector Extraction: After separating basic rotations for one single authentication, to match them with standard feature vectors. As feature based classification of time-series data has a simple model and lower computation, to choose this method for rotation recognitions. First, feature vectors (F-Vectors) for each individual basic rotation are extracted based on their fitting functions created in the previous section. Specifically, to extract the start and end sensory data, the maximal and minimal sensor readings and the corresponding time of these events within one basic rotation for a three-axis accelerometer. A sufficiently large feature vector for use in the authentication protocol. The feature vector will be used to authenticate a key or to directly generate a key, and thus it needs to be of high entropy from an attacker's point of view, i.e. involve a large amount of uncertainty. To argue that shaking is an appropriate movement for creating entropy: it creates varying sensor readings, because it is one of the human movement patterns that includes the highest frequency components. Slower movements will intuitively not generate as much entropy.

C. F-Vector Matching: After extracting feature vectors, then try to match the extracted feature vector with standard feature vectors in the database to recognize a specific basic rotation. Standard feature vectors with given *n* could be mathematically calculated and automatically generated since the acceleration components on three axes represent a trigonometric relationship with acceleration of gravity.

Taking the rotation, after the accelerometer clockwise rotates *π* degrees, the acceleration components *Ax* and *Ay* during such rotation can be calculated as $Ax = Gcos\theta$ and $Ay = Gsin\theta$ ($\theta \in [\alpha, \alpha{+}\pi]$). Therefore, it is easy for users to reset their keys without any modification on access cards. In order to match extracted F-vectors of a basic rotation to standard ones in database, to use Euclidean distance to measure the closeness of these two vectors.

In order to match extracted F-vectors of a basic rotationto standard ones in database, we use Euclidean distance tomeasure the closeness of these two vectors. Specifically weuse following set of equations for three axes:

$$d_x = |\ T_x - S_x\ |$$
$$d_y = |\ T_y - S_y\ |$$
$$d_z = |\ T_z - S_z\ |$$

To identify a basic rotation from the extracted feature vector, we choose the one that has the maximal *R* value for a corresponding standard feature vector.

4 IMPLEMENTATION AND RESULTS

To evaluate the proposed dynamic authentication method, a prototype system is built based on the Intel Wireless Identification and Sensing Platform (WISPs). WISP is a fully-passive ultra high frequency (UHF) RFID tag which integrates an ultra-low-power processor and several low-power sensors such as temperature sensor and accelerometer [6].

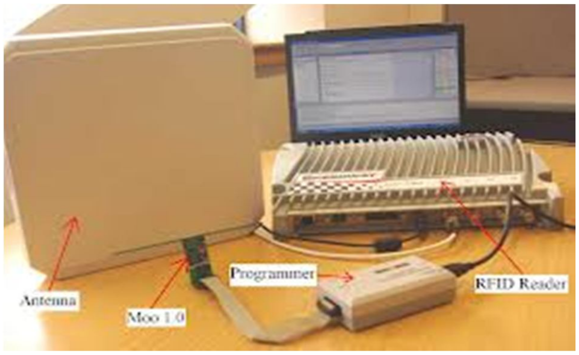


Figure. 5. Antenna-reshaped WISP Tag and Reader

TABLE 1

Accuracy Rate vs. Different Users with Dual Accelerometers (n=4)					
Users	k=1	K=2	K=3	K=4	K=5
User #1	100%	100%	94.%	94.%	96%
User #2	100%	94.%	96.%	100%	98%
User #3	98.%	96.%	94.%	96.%	98%
User #4	96.%	100%	100%	96.%	92%
User #5	100%	100%	94.%	94.%	92%

In figure 5, prototype system, an antenna-reshaped WISP tag equipped with an accelerometer is integrated onto a standard access card [5].

A. Accuracy Rate of the System Authentication: Firstly, a total of 600 basic rotations are performed by one user. The experiment results are summarized in Table 1.

TABLE 2

Accuracy Rate vs. Different k and n

	k = 1	*k* = 2	*k* = 3	*k* = 4	*k* = 5
n = 4	100 %	93.30 %	91.70 %	90.00 %	86.70 %
n = 8	100 %	91.70 %	90.00 %	90.00 %	83.30 %
Delay	1.9s	4.7s	7.7s	10.5s	13.3s

It can be found that as the number of basic rotations *k* and the granularity of rotation recognition *n* increase, the accuracy rate decreases. This is because when the granularity of recognition increases, the likelihood of mismatching two different basic rotations also increases.

Experiments with both single and dual accelerometers are conducted. here is no any surety of availability and back up of data in this environment. In business backup is one of the important consideration.

B. System Performance with Dual Accelerometers: During single-sensor experiments, we observed there exists severe sensory data loss between the WISP and reader. This is because quality of energy harvesting and communication between WISP and reader cannot be always guaranteed during rotation process.

C. System Performance among Different Users: In the first experiment, 50 complex rotations under each number of basic rotations *k* are designated to 5 users.

Experimental results with dual accelerometers are shown in Table 2. Average accuracy rates of all five columns are higher than 95% while in single accelerometer experiment, accuracy rates in 14 of 25 cases are below 90% and the worst case of accuracy rate is as low as 70% which is occurred when user 3 performs a 5 basic-rotation authentication. These experiment results demonstrate our proposed method could increase the key space by more than 30000 times with a high enough accuracy rate of authentication. Besides, accuracy rates among different users are much more stable in Table 2. With dual accelerometers, all accuracy rate variances among five distinct *k* are below 7.5 and average variance of different *k* is 71.8% less than that of single sensor (5.312 vs. 18.816). In below figure 6, shows the further verify the practicability of our system, we conduct experiments among 20 non-technical users.

Results shown in figure 6 fully demonstrate the effectiveness of our system in real life.

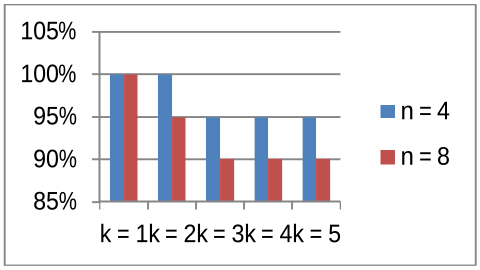


Figure. 6. Experimental results with 20 users

4.1 SIMULATIONS

Simulation results of system performance of our authentication methods are provided in this section. we comprehensively analysis impacts of various environment conditions on the accelerometer-based design which has a more complex authentication algorithm.

A. Impact of Sensory Data Sample Sizes: Sensors powered by harvested RF energy face a severe constraint of energy budget. Higher data sample rate leads to increasing sensor/processor activities and therefore higher energy consumption.

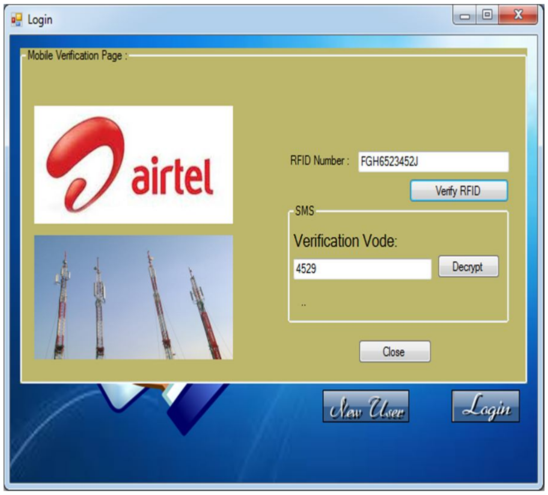
B. Impact of Sensory Data Fractures: Data loss is a common issue in wireless communication. For instance, sensory data between 10*s* and 11.8*s* is lost during one of our experiments. We empirically measured the probability of losing a continuous data block (data fracture) in our prototype with single WISP and results are shown below in TABLE 3 .

TABLE 3

Data Fracture Analysis

Num. of Fracture	0	1	2	3
Existence Ratio	30.00%	50.00%	10.00%	10.00%

From this table, we find the probability of data fracture is higher than non-fracture's (70% vs. 30%). It could be inferred that the occurrence of fracture will increase during long actions as more rotations are continuously performed. we find that our recognition algorithm is fracture-tolerant. In most cases, up to 20% sensory data fracture could be tolerated in systems with little performance degradation. In the user's RFID registration page is showed in below diagram. Which includes the RFID number and mobile verification code itself to be showed in fig 7.



Login

Mobile Verification Page :

RFID Number : FGH6523452J

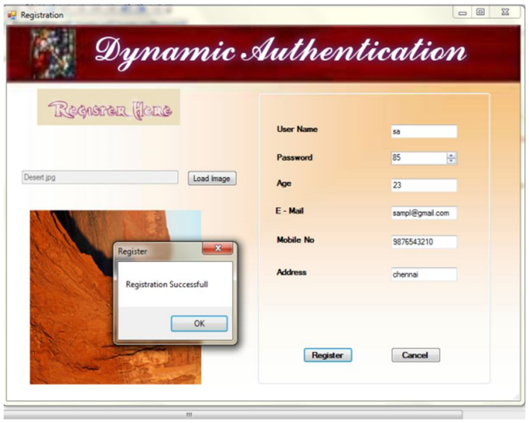
SMS

Verification Vode:

4529

Figure. 7, RFID and mobile code registration page

The user's registration page is contained by the details about the user's information and declared images loading are stored in this page. It showed by the below images fig 8.



Registration

Dynamic Authentication

Register Here

Desert.jpg

User Name: sa

Password: 85

Age: 23

E - Mail: sampl@gmail.com

Mobile No: 9876543210

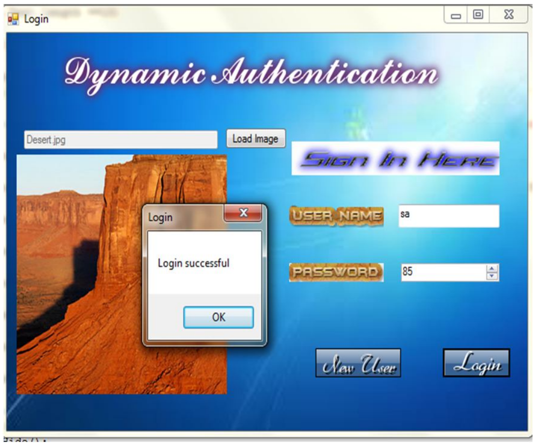
Address: chennai

Register

Registration Successfull

Figure. 8, User's registration page

The user's enter the details and stored to the database. Whenthe user re-enter the system to complete the correct authentication steps to provide the process to correct users.



Login

Dynamic Authentication

Desert.jpg

Sign In Here

USER NAME: sa

PASSWORD: 85

Login

Login successful

Figure. 9, User login page

The user enter the correct information to this system. To verify and validate by the server side database system and authorised user only allow to the access a process.

4.2COMPARISON BETWEEN THE TWO REFERENCE DESIGNS

Different from accelerometer-based design which relies on precise rotations, gyroscope-based design adopts the impulse of the amplitude of the angular velocity (see Section 2). Compared with accelerometer-based design, gyroscope-based design owns a higher authentication accuracy and smaller authentication delay (see Section 4). However, the accelerometer-based design is more robust under changing environmental conditions as the gyroscope-based design is more sensitive to data loss (see Section 5). Both of these two designs have large key space.

5 CONCLUSION

In this paper, we proposes a dynamic authentication with sensory information for the access control systems. Different from existing schemes of authentication in access control systems, which mainly based on static information on cards, our dynamic authentication method combines sensory information from onboard sensors and conventional static ID information. Two case studies of the dynamic authentication are proposed. We theoretically analyses their highly increased key space, which exponentially multiplied static key space in existing authentication methods. To evaluate performance of our design, we built a prototype system and mobile verification code validate authentication mechanism experimentally. In experiments, the proposed authentication algorithm showed a 95% high accuracy rate within different users. In the simulation part, we comprehensively study the impact of sensory data sample size and sensory data loss, which found to be critical factors from experiments on authentication algorithm. Most simulation results validate our algorithm effectively. Growing popularity of electronically based authentication in proximity access control systems calls for a higher security level and greater ubiquity. We believe that authentication bound with dynamic sensory information can effectively enhanced security level of access control systems and will take an important step towards electronically access authentication in the future.

ACKNOWLEDGMENTS

The author would like to thank the management and staff members of the K.Ramakrishnan college of technology for his help and his thoughtful comments.

REFERENCES

[1] Y. Shu, Y. Gu, and J. Chen, “Sensory-Data-Enhanced Authentication for RFID-based Access Control Systems,” in IEEE MASS, 2012.

[2] R. Mayrhofer and H. Gellersen, “Shake well before use: Authenti-cation based on accelerometer data,” Pervasive Computing, pp. 144– 161, 2007.

[3] J. Kong, H. Wang, and G. Zhang, “Gesture recognition model based on 3D accelerations,” in IEEE ICCSE, 2009.

[4] A. P. Sample, D. J. Yeager, and J. R. Smith, “A capacitive touch interface for passive RFID tags,” in IEEE RFID, 2009.

[5] Y. Shu, J. Chen, F. Jiang, Y. Gu, Z. Dai, and T. He, “Demo: WISP-based access control combining electronic and mechanical authentication,” in ACM SenSys, 2011.

[6] M. Buettner and D. Wetherall, “An empirical study of UHF RFID performance,” in ACM MobiCom, 2008.