On The Security of An Efficient Dynamic Auditing Protocol in Cloud Storage

S.Adhikesavan
Assistant Professor
Department of Information Technology
Ganadipathy Tulsi's Jain Engineering College, Vellore

N.Sathish
Assistant Professor
Department of Information Technology
Panimalar Engineering College, Chennai

Abstract

Automated teller machines (ATMs) are well known devices typically used by individuals to carry out a variety of personal and business financial transactions and/or banking functions. ATMs have become very popular with the general public for their availability and general user friendliness. ATMs are now found in many locations having a regular or high volume of consumer traffic. For example, ATMs are typically found in restaurants, supermarkets, Convenience stores, malls, schools, gas stations, hotels, work locations, banking centers, airports, entertainment establishments, transportation facilities and a myriad of other locations. ATMs are typically available to consumers on a continuous basis such that consumers have the ability to carry out their ATM financial transactions and/or banking functions at any time of the day and on any day of the week. Access card authentication is critical and essential for many modern access control systems, which have been widely deployed in various government, commercial, and residential environments. However, due to the static identification information exchange among the access cards and access control clients.

Keywords: Authentication, Sensory Data, Access Control System, Wireless Rechargeable Sensor

I. INTRODUCTION

Access control is a mechanism that enables an authority to control access to restricted areas and resources at a given physical facility or computer-based information system. 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 dialed. Due to the physical constraints of mechanical matching systems, they are insufficient to meet the demanding requirements of access control authentication for critical infrastructures. On the other hand, it is also very hard to frequently change the interior structure of such matching mechanisms for security enhancement.

The other category of authentication for access control systems is electronic authentication including barcode, magnetic stripe, biometrics, and so on. Compared with mechanical matching authentications, the electronic authentications such as RFID-based smart card offer much more convenience and flexibility for both administrators and users of access control systems. However, it still suffers from similar problem of key loss because authentication is only based on the encoded identification data on the card. Anyone who carries the card will be granted the access and the security of the system still can be compromised.

To further enhance the security of access control systems, various biometric authentication mechanisms have been introduced to identify the authorized personnel. Although these biometric authentication methods such as fingerprint, iris, and voice recognitions are able to provide personal identification, they have high infrastructure cost and access privileges cannot be transferred among trusted users.

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 with backward compatibility. Specifically, we add dynamic data into the traditional authentication information by using sensors such as accelerometer, gyroscope, and so on. This authentication framework is adaptive to the change of encryption complexity of the access control systems and could be adopted with minor modification of existing infrastructure. In summary, on top of the previous conference paper [1], 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 demonstrate the proposed framework with two case studies and theoretically prove that our dynamic authentication significantly increases the key space for proximity authentication systems with the integration of low-cost sensors.
- We have fully implemented and built a running prototype of the proposed dynamic authentication framework 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 real-world settings.

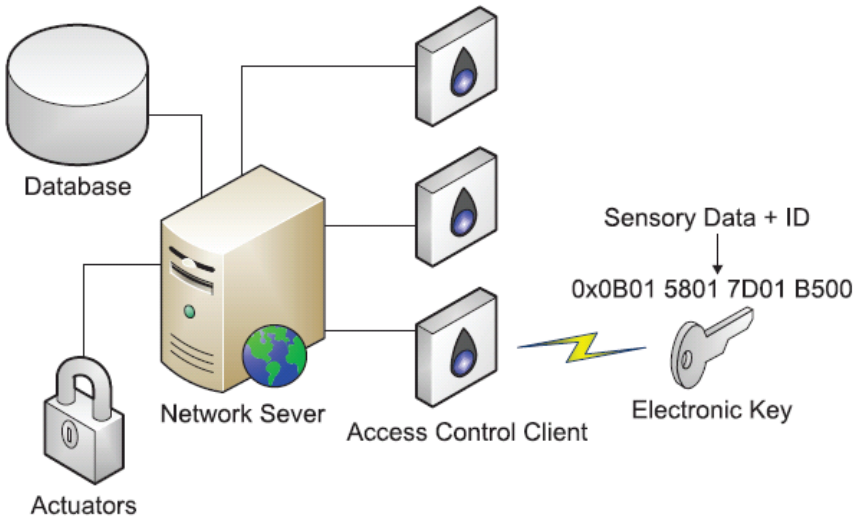


Fig. 1: System Function DIAGRAM

The remainder of this paper is organized as follows: First we propose the dynamic authentication framework with sensory information in Section 2. We then provide authentication algorithms of our system in Section 3. System working performance and simulations of the authentication method are shown in Sections 4 and 5. Comparison between the proposed two reference designs is given in Section 6. We discuss related work in Section 7 and conclude in Section 8.

II. DESIGN OF THE DYNAMIC AUTHENTICATION WITH SENSORY INFORMATION

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. In this work, we 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 our system design is shown in Fig. 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 an 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, we successfully remove the system vulnerable period between loss/stolen of access card and the deactivation of the card after users' report. 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, 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. In fact, because we 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 our authentication method [2], [3], [4], and therefore deal with several security vulnerabilities such as replay attack and eavesdropping.

The identification information on access cards normally are static. With the addition of dynamic sensory data from onboard sensors, we are able to significantly increase the security key space P and hence the security level for existing electronic authentication systems. A wide variety of sensors including accelerometer, gyroscope, and so on can be used in our system. To illustrate the basic concept and the resulting security enhancement of our sensory data enhanced access control system design, we use both three-axis accelerometer and gyroscope as examples in the following sections. In particular, we utilize the sensory data generated from the rotation of accelerometer and gyroscope to introduce reference designs for the proposed sensory data enhanced authentication scheme. Through our prototyping system and real-world experiments, we demonstrate such a rotation-based design is a feasible and practical option for the proposed generic dynamic authentication framework.

A. Accelerometer-Based Reference Design

1) *Two-Dimensional Rotation*

For an accelerometer, if it is being rotated, the static acceleration of gravity on its three axes will change accordingly. For a two-dimensional rotation, we can calculate the tilt angle alpha of an accelerometer from static acceleration of gravity on its X- and Y -axes to determine the position of the accelerometer in a two-dimensional plane.

In Fig. 2, we illustrate a simple example on how to determine the position of an accelerometer. In Fig. 2, A_x and A_y are acceleration components of gravity on X- and Y - axes, respectively. The tilt angle _ can then be calculated by equation A_x ¼ Gcos_ and A_y ¼ Gsin_, where G is the static acceleration of gravity. We define the most basic rules and parameters for two-dimensional rotations, which can be used to express more complex rotation actions:

Basic rotation rules:

- For all rotations, they are two dimensional.
- The basic rotation is omnidirectional, either clockwise or counterclockwise.
- The new rotation starts from the end position of the previous one.
- Any single basic rotation does not exceed 2_degrees.

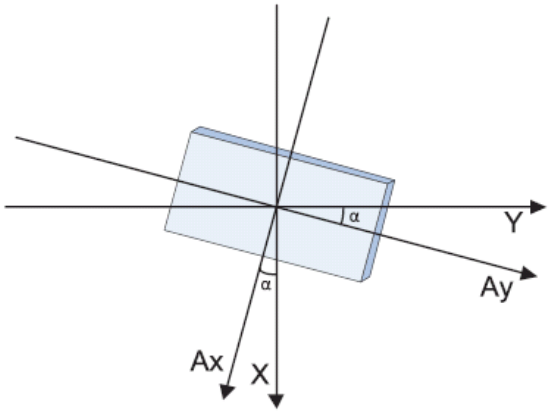


Fig. 2: Accelerometer Rotation Example

Basic rotation parameters:

The Number of Basic Rotations k. The number of basic actions performed in one rotation sequence. Basic rotation number reveals the complexity of encryption.

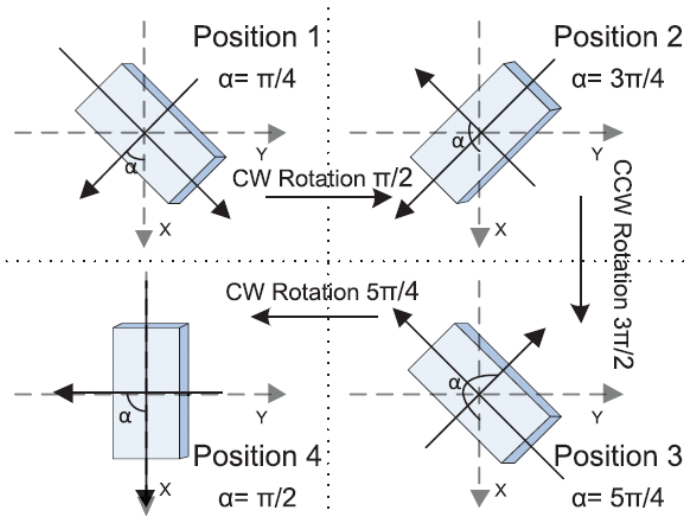
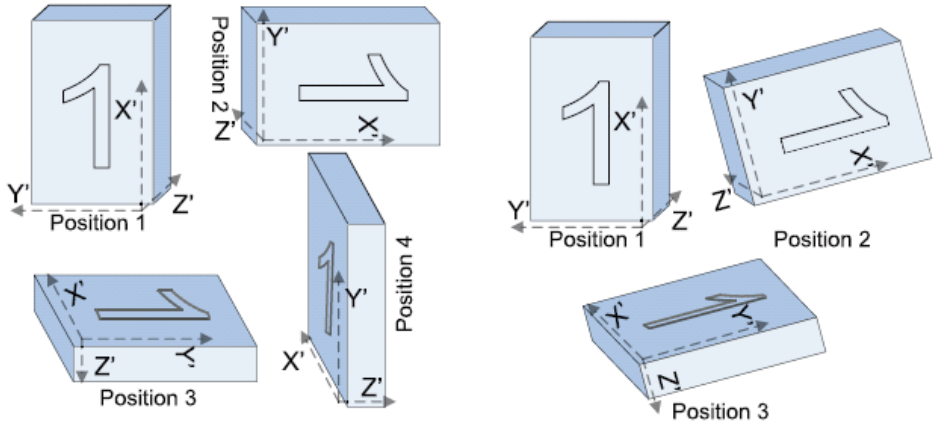


Fig. 3: Rotation Sequence Diagram (2D)

Fig. 3 shows an example of rotation sequence with three basic rotations (k = 3) and granularity of the recognition n ¼ 8. CW and CCW in Fig. 3 denotes clockwise and counterclockwise, respectively.



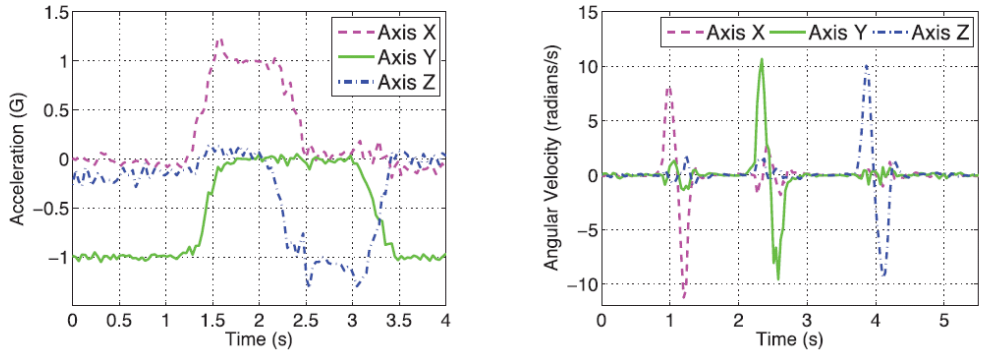
(a) Valid 3D Rotation (b) Invalid 3D Rotation

Fig. 4: Rotation Sequence Diagram (3D)

2) *Three-Dimensional Rotation*

In this part, we extend our design to rotations in three-dimensional space. Since determining the attitude of sensor solely based upon static acceleration of gravity is impossible (imagine standing and holding your cell phone face to you, the values of accelerometer at cell phone will not change if you turn from the west to the north). Based on the relative positions of the accelerometer and the ground, we extend the basic two-dimensional rotation rules for three-dimensional rotations: 1) During the whole rotation process, either plane XY, YZ or XZ under the coordinate of accelerometer is perpendicular to the ground 2) Accelerometer only rotates in one plane under its own coordinate (XY, XZ or YZ) during one basic rotation; 3) Rotation in a different plane is allowed if one axis among _X, _Y or _Z of the accelerometer is perpendicular to the ground at the end of the previous basic rotation.

Fig. 4a demonstrates an example of a 3D rotation sequence follows the rules above with k ¼ 3 basic rotations. We coplot the coordinate of the accelerometer to illustrate 3D rotations. In Fig. 4a, each action between two con-secutive 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. For example, Position 2 rotates to Position 3 in Fig. 4b is prohibited while Position 1 rotates to Position 2 in Fig. 4a is likely to happen if the granularity of the rotation recognition n ¼ 4.



(a) 3D Rotations of an Accelerom-eter (b) Standard Rotations of a Gyro-scope

Fig. 5: Sample Data of Rotations of Accelerometer And Gyroscope

Corresponding sample data of this three-dimensional rotation are shown in Fig. 5a. In Fig. 5a, it could be found that values at each axis of the accelerometer change in different ways during the rotation process, therefore, offer great opportunities for sensory information-based authentication design.

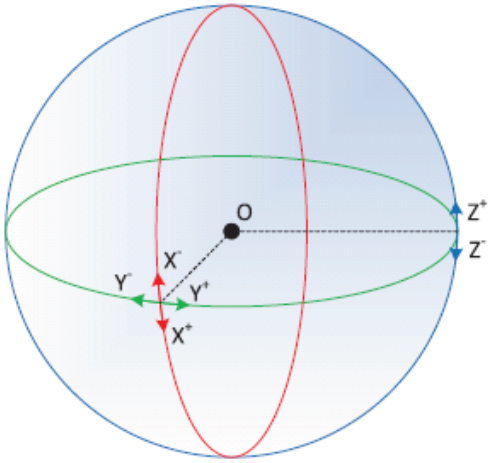


Fig. 6: Standard Rotations of A Gyroscope

B. 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 because it returns the angular velocity on each axis simultaneous when rotating. Imaging there is a ball with center of O, Fig. 6 depicts six standard rotations of the ball using vectors. Corresponding sensory data of the six basic rotations of a typical three-axis gyroscope is shown in Fig. 5b.

Different from accelerometer-based design that relies on precise rotations, higher rotation speed of the gyroscope leads to a higher output value that make it easier for authentication. It can be seen in Fig. 5b that different standard rotations of a gyroscope can be easily differen-tiated from when the gyroscope remains standstill through the amplitude of the angular velocity. In this gyroscope-based reference design, we only use such binary rotation information (whether rotated) at each axis to perform sensory-data-based authentication.

III. ROTATION RECOGNITION

In the previous section, we discuss the potential of large key space increase for our dynamic authentication with sensory information design. In this section, we further elaborate on the detailed sensor rotation recognition algorithms.

By comparing the sample data of accelerometer (Fig. 5a) and gyroscope (Fig. 5b), we find that output of the accelerometer exhibits a more complex behavior. This is because gyroscope measures the angular velocity and tends to generate impulses during one single basic rotation, which could be treated as a special case of the output of the accelerometer. Therefore, in this section, we use the sensory data of accelerometer to illustrate the whole rotation recognition algorithms and discuss how to deal with the sensory data of gyroscope in Section 3.4.

One complete dynamic authentication process consists of a sequence of basic rotations. To accurately identify each individual basic rotation from raw accelerometer data, we perform following three operations in the network server.

A. Data Preprocessing

The first step of rotation recognition is data preprocessing. The main goals are to separate and filter each individual basic rotation from a series of raw accelerometer data.

To separate the individual basic rotations, we 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. To accurately recognize such pauses and separate different basic rotations, we adopt a sliding window approach. In this approach, the accelerometer readings in the first t_w 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 (one in our implementation), we 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 t_s seconds, with t_s duration of new data appended to the end of the sliding window while the first t_s duration of sensory data are discarded. Empirically, we set t_w = 1 s and t_s = 0:3 s in our system implementation. In this way, we have achieved accurate separation of basic rotations in one complete authentication. To visualize above data preprocessing step, Fig. 7 shows one authentication with four basic rotations that performed slowly on our prototype implementation. The shaded regions represent sliding windows at three pauses. Clearly from Fig. 7, it can be found that the accelerations on three axes of the accelerometer are rather stable during pauses between different basic rotations.

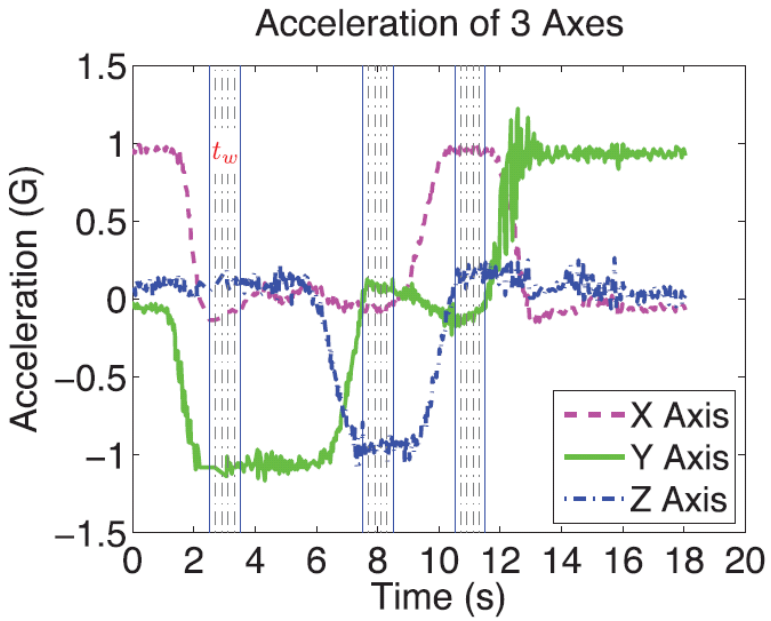


Fig. 7: Example Sensory Data of A 3D Rotation

After identifying pauses between basic rotations, we then use least square estimation to fit the raw readings for each individual basic rotation from the accelerometer.

B. Feature Vector Extraction

After separating basic rotations for one single authentica-tion, we match them with standard feature vectors. As feature-based classification of time-series data has a simple model and lower computation, we choose this method for rotation recognitions. First, feature vectors (F-vectors) for each individual basic rotations are extracted based on their fitting functions created in the previous section. Specifi-cally, we extract the start and end sensory data, the maximal and minimal sensor readings, and the corre-sponding time of these events within one basic rotation. Then, for a three-axis accelerometer, we can represent their feature vectors using the following set of equations:

C. F-Vectors Matching

After extracting feature vectors, we then try to match them 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.

D. Discussion of Gyroscope-Based Design

Since a rotation process in gyroscope-based design also consists of several basic rotations, the first operation of data pre-processing presented in Section 3.1 can be used without any modification. In feature vector extraction, we only need to extract the maximal sensor readings on each axis because there is only one impulse during a basic rotation. After constructing the standard feature vectors of limited rotations of the gyroscope (e.g., six standard rotations), F-vector matching can be accomplished identically to the accelerometer based design.

Note that methodology of rotation recognition is not limited to the feature-based classification. For example, one can calculate distance between sensory measurements and sensory data of standard rotations through dynamic time warping to recognize basic rotations, and online learning of the timing parameters in the data preprocessing step could also use to improve the recognition performance. In addition, methodologies used in gesture recognition can also be borrowed [5], [6], [7], [8]. Although they may have higher computation complexity, they will not affect the essence of the dynamic authentication framework.

IV. TESTBED EVALUATION

To evaluate the proposed dynamic authentication method, a prototype system is built based on the Intel Wireless Identification and Sensing Platform [9]. WISP is a fully passive ultrahigh-frequency (UHF) RFID tag that integrates an ultralow-power processor and several low-power sensors such as temperature sensor and accelerometer. Through WISP's antenna, the signal from standard UHF RFID readers can be used for both communication and powering the entire WISP [10].

In the prototype system, an antenna-reshaped WISP tag equipped with an accelerometer is integrated onto a standard access card. WISP tags we use are backward-compatible with existing RFID standards and hardware. Therefore, they can be powered and read by any unmodified, commercially available UHF RFID readers.

Since the current WISP does not have an embedded gyroscope, we test the accelerometer-based design exclusively on the prototype system. However, by modifying the hardware, gyroscope can be integrated onto WISP as well. In this paper, we

conduct experiments on an iPhone 4 to evaluate the gyroscope-based design and summarize the authentication results in Appendix B, available in the online supplemental material.

Fig. 8: Antenna – Reshaped WISP Tag And Reader

A. Evaluation of the Accelerometer-Based Design

Both authentication accuracy and delay are two most essential factors for practical access control systems. In this section, we comprehensively study the accuracy of our rotation recognition algorithm on identifying a series of basic rotations performed by users for system authentication with one single accelerometer. Specifically, we define accuracy rate of the system authentication as the percentage of complex rotations that have been correctly recognized for system authentication algorithm. During the experiment, we also record rotation delay which refers to the duration of a complete action and the accuracy rate of authentication with varying number of basic rotations k under two different granularity of recognition n. In experiments, predefined rotations are randomly generated by the computer and then performed by users. Due to the space constraint, we only present two-dimensional authentication evaluation and analysis in the main file. Experimental results of three-dimensional rotations can be found in Appendix C, available in the online supplemental material.

V. COMPARISON BETWEEN THE TWO REFERENCE DESIGNS

Different from accelerometer-based design that relies on precise rotations, gyroscope-based design adopts the impulse of the amplitude of the angular velocity (see Section 2.2). 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.

VI. CONCLUSIONS

In this paper, we propose 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 analyze 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 validate authentication mechanism experimentally. In experiments, the proposed authentication algorithm showed a 95 percent high accuracy rate among 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 toward electronically access authentication in the future.

REFERENCES

[1] Y. Shu, Y. Gu, and J. Chen, "Sensory-Data-Enhanced Authentica-tion for RFID-Based Access Control Systems," Proc. IEEE Ninth Int'l Conf. Mobile Ad Hoc Sensor Systems (MASS), 2012.
[2] A. Juels, "RFID Security and Privacy: A Research Survey," IEEE J. Selected Areas Comm., vol. 24, no. 2, pp. 381-394, Feb. 2006.
[3] R. Mayrhofer and H. Gellersen, "Shake Well Before Use: Authentication Based on Accelerometer Data," Proc. Fifth Int'l Conf. Pervasive Computing, pp. 144-161, 2007.

[4] M. Burmester, T.V. Le, B.D. Medeiros, and G. Tsudik, "Uni-versally Composable RFID Identification and Authentication Protocols," ACM Trans. Information and System Security, vol. 12, no. 4, article 21, 2009.
[5] J. Kong, H. Wang, and G. Zhang, "Gesture Recognition Model Based on 3D Accelerations," Proc. IEEE Fourth Int'l Conf. Computer Science & Education (ICCSE), 2009.
[6] S. Mitra and T. Acharya, "Gesture Recognition: A Survey," IEEE Trans. Systems, Man and Cybernetics, vol. 37, no. 3, pp. 311-324, May 2007.
[7] S. Zhou, Q. Shan, F. Fei, W.J. Li, C.P. Kwong, P.C.K. Wu, B. Meng, C.K.H. Chan, and J.Y.J. Liou, "Gesture Recognition for Interactive Controllers Using MEMS Motion Sensors," Proc. IEEE Fourth Int'l Conf. Nano/Micro Engineered Molecular Systems (NEMS), 2009.
[8] T. Park, J. Lee, I. Hwang, C. Yoo, L. Nachman, and J. Song, "E-Gesture: A Collaborative Architecture for Energy-Efficient Gesture Recognition with Hand-Worn Sensor and Mobile Devices," Proc. Ninth ACM Conf. Embedded Networked Sensor Systems (SenSys), 2011.
[9] A.P. Sample, D.J. Yeager, P.S. Powledge, A.V. Mamishev, and J.R. Smith, "Design of an RFID-Based Battery-Free Program-mable Sensing Platform," IEEE Trans. Instrumentation and Measurement, vol. 57, no. 11, pp. 2608-2615, Nov. 2008.
[10] M. Buettner and D. Wetherall, "An Empirical Study of UHF RFID Performance," Proc. ACM MobiCom, 2008.
[11] A.P. Sample, D.J. Yeager, and J.R. Smith, "A Capacitive Touch Interface for Passive RFID Tags," Proc. IEEE Int'l Conf. RFID, 2009.
[12] N. Saxena and J. Voris, "Still and Silent: Motion Detection for Enhanced RFID Security and Privacy without Changing the Usage Model," Proc. Sixth Int'l Conf. Radio Frequency Identification: Security and Privacy Issues, vol. 6370, pp. 2-21, 2010.
[13] D. Ma and N. Saxena, "A Context-Aware Approach to Defend against Unauthorized Reading and Relay Attacks in RFID Systems," Security and Comm. Networks, doi: 10.1002/sec.404, Dec. 2011.
[14] N. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. Campbell, "A Survey of Mobile Phone Sensing," IEEE Comm. Magazine, vol. 48, no. 9, pp. 140-150, Sept. 2010.
[15] P. Kannan, P. Seshadri, M.-C. Chan, A.L. Ananda, and L.-S. Peh, "Low Cost Crowd Counting Using Audio Tones," Proc. 10th ACM Conf. Embedded Network Sensor Systems (SenSys), 2012.
[16] J. Chung, M. Donahoe, C. Schmandt, I.-J. Kim, P. Razavai, and M. Wiseman, "Indoor Location Sensing Using Geo-Magnet-ism," Proc. ACM Ninth Int'l Conf. Mobile Systems, Applications, Services (MobiSys), 2011.
[17] Y. Shu, J. Chen, F. Jiang, Y. Gu, Z. Dai, and T. He, "Demo: WISP-Based Access Control Combining Electronic and Mechanical Authentication," Proc. ACM Conf. Embedded Network Sensor Systems (SenSys), 2011.