ISSN: 2348-2079

MAY-2015

International Journal of Intellectual Advancements and Research in Engineering Computations

SECURITY ENHANCEMENT FOR ACCESS CONTROL SYSTEMS BY USING DYNAMIC AUTHENTICATION

[1]M.P. Aarthi, [2]S.M. Karpagavalli.

ABSTRACT

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, 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 and iris identification can further identify the user who is requesting authorization, they incur high system costs and access privileges cannot be transferred among trusted users.

In this work, introducing a dynamic authentication with sensory information for the access control systems. By combining sensory information obtained from onboard sensors on the access cards as well as the original encoded identification information are able to effectively tackle the problems such as access card loss, stolen, and duplication.

Our solution is backward-compatible with existing access control systems and significantly increases the key spaces for authentication. Theoretically demonstrate the potential key space increases with sensory information of different sensors and empirically demonstrate simple rotations can increase key space by more than 1,000,000 times with an authentication accuracy of 90 percent. It performed extensive simulations under various environment settings and implemented our design on WISP to experimentally verify the system performance.

INTRODUCTION

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals.

Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user

Author for Correspondence:

[1]Final year ME, Al-Ameen Engineering College, Erode, Tamilnadu, India

[2]Assistant Professor/CSE, Al-Ameen Engineering College, Erode, Tamilnadu, India

name —i.e. the password-this is sometimes termed one-factor authentication. With two factor authentication, something the user 'has' is also used; and with three-factor authentication, something the user 'is' is also used.

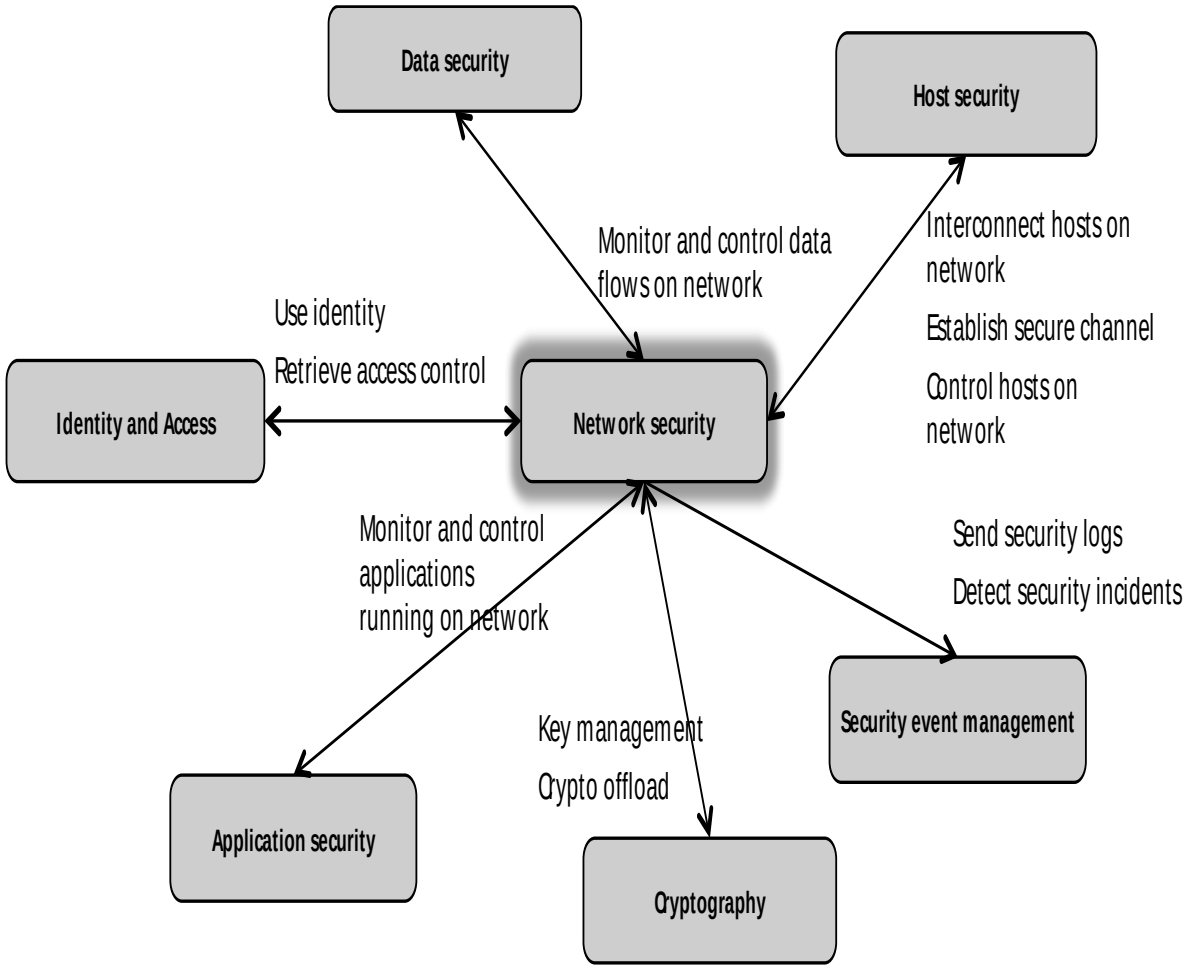

Figure.1.1. Network Security Relationship

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) helps detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

and traffic for network may be logged for audit purposes and for later high-level analysis.

Communication between two hosts using a network may be encrypted to maintain privacy. Honey pots, essentially decoy network-accessible resources, may be deployed in a network as surveillance and early-warning tools, as the honey pots are not normally accessed for legitimate purposes. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis may be used to further tighten security of the actual network being protected by the honey pot.

RELATED WORK

Recently, researchers have introduced several RFID-based solutions to improve the security level of access control systems. Sample et al. [1] present a solution for adding capacitive touch sensing onto RFID tags for capacitive user input. To further improve the system security, Saxena and Voris [2] introduce a method to generate random numbers to achieve motion detection based on the ambient noise of onboard accelerometer of RFID tags. In [3], by utilizing on-board sensors, authors design multiple context-aware selective unlocking mechanisms to prevent unauthorized reading and replay attacks.

The most similar paper to this work is the "RFIDs and secret handshakes" [4]. In this work, based on WISP, authors introduce an approach to tackle the ghost-and-leech attack between contactless cards and readers. Specifically, authors propose a context-aware authentication method by allowing contactless cards to communicate with readers only if the card owner performs a secret handshake. However, different from this quasi-biometrical authentication method that relies on the unique user patterns exhibited during the authentication process, we proposed an orthogonal solution which has a large key space increase by combining dynamic sensory information and static identifier during authentication process. By doing so, our method is also compatible with the context-aware solution.

Although currently there exist several sensor-aided solutions to improve the security of access control systems, they have relatively small improved key space and operate in limited environment settings. Different from previous approaches, in our proposed design, we ensure that the dynamic authentication framework with sensory information combines the best of mechanical and electronic authentication methods which is backward compatible with the existing deployed RFID authentication systems. Apart from the accelerometer and gyroscope, various low power sensors including temperature, microphone, electronic compass and barometer [5], [6], [7] are also desirable candidates of the proposed framework that would bring large key space increases with simple sensor readings. In addition, trusted users can share and reset access privilege among themselves. With such embedded sensor information and significantly increased key space, we can effectively counterattack the compromises of the access control system.

DYNAMIC AUTHENTICATION WITH SENSORY INFORMATION

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 [9]. 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. 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. It still suffers from similar problem of key loss because authentication is only based on the encoded identification data on the card.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

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 [8], 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.

PROBLEM STATEMENT

Access card authentication is critical and essential for many modern access control systems, which have been widely deployed in various governments, commercial and residential environments. Access control systems can be divided into two broad categories. The first category is based on mechanical matching, such as keys and combination locks. 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. Electronic authentication including barcode, magnetic stripe, biometrics and etc.

Although advanced biometric authentication methods such as fingerprint and iris identification can further identify the user who is requesting authorization, they incur high system costs and access privileges cannot be transferred among trusted users. A novel electronic proximity authentication framework that enhances the security level of existing RFID-based access control systems with backward compatibility. The following problems are identified in the current security methods.

- Stolen or unauthorized duplications of the access cards
- Sensors on the access cards effectively tackle the problems such as access card loss, stolen and duplication
- High system costs and access privileges cannot be transferred among trusted users.

AUTHENTICATION AND ACCESS CONTROL

Authentication and access control measures should ensure appropriate access to information and information processing facilities – including mainframes, servers, desktop and laptop clients, mobile devices, applications, operating systems and network services – and prevent inappropriate access to such resources.

ACCESS CONTROL POLICY

An access control policy should be established, documented and periodically reviewed, based on business needs and external requirements. Access control policy and associated controls could

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

take account of: Security issues for particular data systems and information processing facilities, given business needs, anticipated threats and vulnerabilities; Security issues for particular types of data, given business needs, anticipated threats and vulnerabilities;

Access control policies generally should include clearly stated rules and rights based on user profiles, consistent management of access rights across a distributed/networked environment, an appropriate mix of administrative, technical and physical access controls administrative segregation of access control roles, requirements for formal authorization of access requests; and Requirements for authorization and timely removal of access rights. Policies should include a focus on ensuring authorized user access, and preventing unauthorized user access, to information and information systems. This could include: formal procedures to control the allocation of access rights, procedures covering all stages in the life-cycle of user access, from provisioning to de-provisioning; and special attention to control of privileged access rights.

PRIVILEGE AND USER ACCESS TOKEN MANAGEMENT

Allocation and use of access privileges should be restricted and controlled. This could include: development of privilege profiles for each system, based on intersection of user, profiles and system resources, granting of privileges based on these standard profiles when possible, a formal authorization process for all privileges, with additional review, requirements for exceptions to standard profiles and maintaining a current record of privileges granted. Allocation of access tokens key-cards should be controlled through a formal management process. This could include: requiring users to sign a statement indicating they will keep their access tokens secure, secure methods for creating and distributing tokens, use of two-factor tokens where appropriate and technically feasible, development of procedures to verify a user's identity prior to providing a replacement token and Prohibiting "loaning" of tokens.

POLICY ON USE OF NETWORK SERVICES

Users should be provided with access only to the network services that they have been specifically authorized to use. This could include: authorization procedures for determining who is allowed to access to which networks and network services, consistent with other access rights and Policies on deployment of technical controls to limit network connections. Physical and logical access to diagnostic and configuration ports should be appropriately controlled. This could include: Physical and technical security for diagnostic and configuration ports and Disabling/removing ports, services and similar facilities which are not required for business functionality Where appropriate and technically feasible, groups of information users and services should be segregated on networks. This could include Separation into logical domains, each protected by a defined security perimeter and Secure gateways between/among logical domains.

NETWORK CONNECTION CONTROL

Capabilities of users to connect to the network should be appropriately restricted, consistent with access control policies and applications requirements. This could include Filtering by connection type and Additional authentication access control measures as appropriate, Positive source and destination address checking and Routing limitations based on the access control policy. Controls should be implemented to restrict operating system access to authorized users, by requiring authentication of authorized users in accordance with the defined access control policy. This could include: providing mechanisms for authentication by knowledge-, token- and/or biometric-factor methods as appropriate, recording successful and failed system authentication attempts, recording the use of special system privileges; and Issuing alarms when access security controls are breached.

USER IDENTIFICATION AND AUTHENTICATION

All system users should have a unique identifier for their personal use only. A suitable authentication technique – knowledge-, token- and/or biometric-based – should be chosen to authenticate the user. This could include: shared user-IDs are employed only in exceptional circumstances, where there is a clear justification, generic user-IDs are employed only where no individual-user-level audit is required and limited access privileges otherwise

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

justify the practice and strength of the identification and authentication methods are suitable to the sensitivity of the information being accessed.

SESSION TIME CONTROL

Interactive sessions should shut down and "lock out" the user after a defined period of inactivity. Resumption of the interactive session should require re-authentication. This could include: Time-out periods that reflect risks associated with type of user, setting of use and sensitivity of the applications and data being accessed and Waiver or relaxation of time-out requirement when it is incompatible with a business process provided other steps are taken to reduce vulnerabilities.

Restrictions on connection times should be used to provide additional security for high-risk applications or remote communications capabilities. This could include: requiring re-authentication at timed interval, restricting overall connection duration or connection time period and restricting connection locations. Sensitive systems should have a dedicated computing environment. This could include: explicit identification and documentation of sensitivity by each system/application controller, construction of appropriately isolated environments where technically and operationally feasible and Explicit identification and acceptance of risks when shared facilities and/or resources must be used.

DYNAMIC AUTHENTICATION SCHEME FOR ACCESS CONTROL SYSTEMS SECURITY

Dynamic data into the traditional authentication information by using sensors such as accelerometer, gyroscope and etc. 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. Dynamic authentication significantly increases the key space for proximity authentication systems with the integration of low-cost sensors. It is fully implemented and built a running prototype of the proposed dynamic authentication framework. The Intel Wireless Identification and Sensing Platform (WISP). Based on the running prototype extensively evaluated our design in terms of system accuracy and usability in the real-world settings. The identification information on access cards normally is static. The addition of dynamic sensory data from onboard sensors, 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 our system. System Implementation has the following phases:

- Enrollment Phase
- Rotation Recognition
  - (i) Data Pre-Processing
  - (ii) Feature Vector Extraction
  - (iii) F-Vectors Matching
- Server verification
- Accessing service

ENROLLMENT PHASE

The aim of this phase is to allow a user and a server to negotiate a shared secret to authenticate succeeding logins for this user. The user begins using Accelerometer sensor for the Access Control Systems.

ROTATION RECOGNITION

Dynamic authentication with sensory information design. In this section further elaborate on the detailed sensor rotation recognition algorithms. By comparing the sample data of accelerometer find that output of the accelerometer exhibits a more complex behavior.

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.

FEATURE VECTOR EXTRACTION

After separating basic rotations for one single authentication match them with standard feature vectors. As feature based classification of

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

time-series data has a simple model and lower computation 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 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.

F-VECTORS 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.

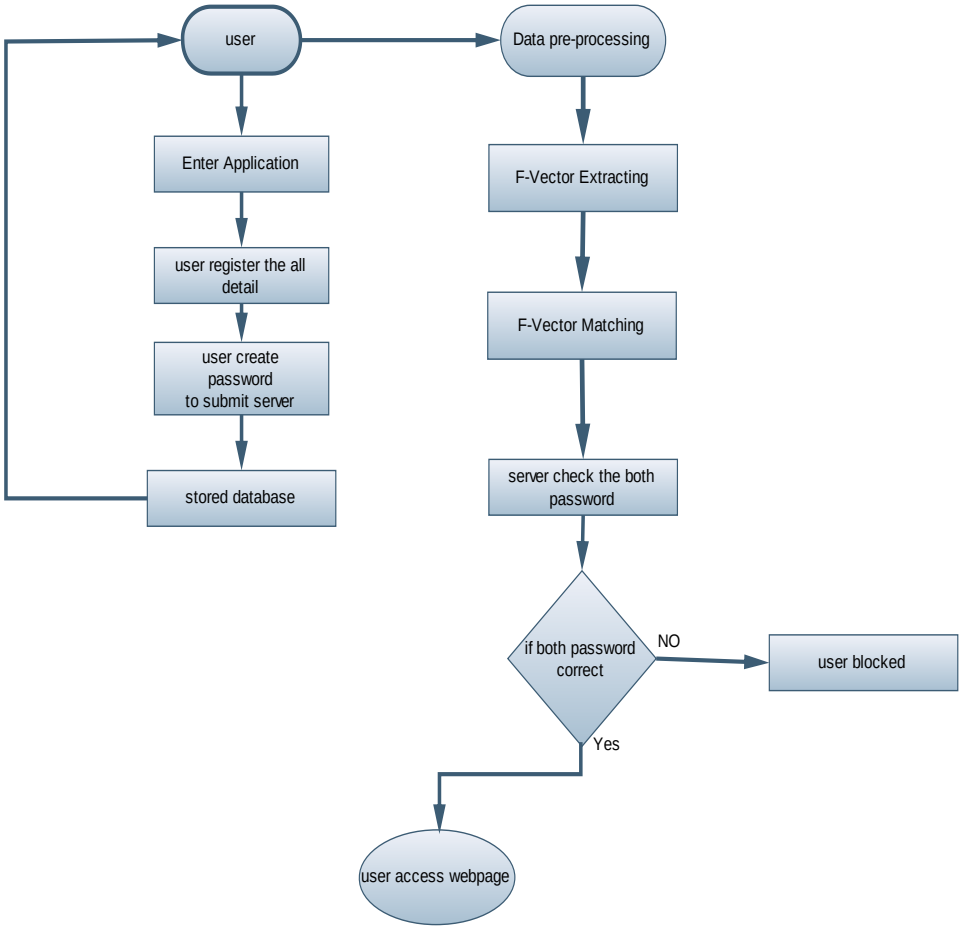

Fig. No: 6.1. Dynamic Authentication Scheme for Access Control Systems Security

SERVER VERIFICATION

Server can verify the authenticity of the registration details and then obtain with the key. Server also compares the source of received key. Then server verifies both password, the password match or not.

ACCESSING SERVICE

User enter the browser and Register to server then server through mail on password then user receive the mail and send to server .then server verify both password, if correct the password open the view all detail ,else if not match that password means you won't allow the site inside.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

CONCLUSION

The sytem supports user authentication and access control mechanism for the network data access services. Backward-compatible with existing access control systems and significantly increases the key spaces for authentication. The potential key space increases with sensory information. Secure Registration and Recovery operations are efficiently handled in the system. The system supports key space by more than 1, 000, 000. The system achieves authentication accuracy of 90%. Implemented our design on wisp to experimentally verify the system performance.

REFERENCES

[1]. 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.

[2]. 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.

[3]. 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.

[4]. A. Czeskis, K. Koscher, J.R. Smith, and T. Kohno, "RFIDs and Secret Handshakes: Defending against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications," Proc. 15th ACM Conf. Computer and Comm. Security (CCS), 2008.

[5]. 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.

[6]. 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.

[7]. J. Chung, M. Donahoe, C. Schmandt, I.-J. Kim, P. Razavai, and M. Wiseman, "Indoor Location Sensing Using Geo-Magnetism," Proc. ACM Ninth Int'l Conf. Mobile Systems, Applications, Services (MobiSys), 2011.

[8]. Y. Shu, Y. Gu, and J. Chen, "Sensory-Data-Enhanced Authentication for RFID-Based Access Control Systems," Proc. IEEE Ninth Int'l Conf. Mobile Ad Hoc Sensor Systems (MASS), 2012.

[9]. Yuanchao Shu, Yu (Jason) Gu and Jiming Chen, "Dynamic Authentication With Sensory Information For The Access Control Systems", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com