ACIT'2017
The International Arab Conference on Information Technology
Yassmine Hammamet, Tunisia
December 22-24, 2017

Enhanced Multi-keyed Risk Adaptive Hybrid RFID Access Control System

Malek Al-Zewairi, Salam Hamdan and Mustafa Al Fayoumi
Princess Sumaya University for Technology, Jordan

***Abstract*—the traditional access control system has been proven inefficient in dealing with modern systems where the access decision might be influenced by several factors. Several works have to be done on next-generation access control systems where risk plays a crucial role in the access control making the decision, which has led to propose several risk adaptive/aware access control models. In this paper, an enhanced multi-keyed model for generating the symmetric encryption key dynamically on the fly is proposed. The experimental results show that the proposed model has improved the overall security while preserving the same architecture of the previous model.**

Keywords— RFID; Access Control; Risk; Fuzzy Logic;

I. INTRODUCTION

Protecting the entry points will prevent the unauthorized users to access the resources and that will be achieved by using the access control system. The access control system should be adaptable to the dynamic changes; however, the traditional access control is not. In order to deal with the dynamic changes, the risk-based access control system is used therefore it is able to accommodate the permissions according to various factors that could depend on the time, the situation, the environment or the operation [1, 2]. Using the risk adaptive access control models will guarantee to acquire the equilibrium of granting or revoking the permissions while keeping the system's security high [2].

Nowadays the objects are identified automatically by using a technology called Radio Frequency Identification (RFID). A RFID tag usually is attached to an item and it sends the item's information upon requests such as ID, name and so on. The RFID tag can be used for example in warehouses, it can issue warnings if any of the goods is expired or almost will be expired. Another example of using the RFID is using it in the washing machines; the RFID tags would give information about laundry and help the washing machine to decide the cycle's times and the water temperature. The communication between the tags and the readers are wireless and there is no need for physical connection. The RFID system is commonly used in access control application where there is a backend database that is storing the information of the access control system [3].

The risk factor estimation is imprecise therefore, the risk factors are uncertain. Due to this uncertainty, the Fuzzy Inference Systems (FIS) is implemented in risk-based access control systems [4–10].

In this paper, the authors enhanced their previous work on Risk adaptive hybrid RFID access control system. The same system architecture proposed in [4] is used in the proposed model. Nonetheless, unlike the previous model, the proposed model utilizes a multi-keyed model to generate the symmetric encryption key dynamically on the fly. The proposed model enhances the security, as the compromise of any tag will not affect the whole system.

The rest of this paper is organized as follows: Section 2 discusses the different works done on this subject. Section 3 highlights the security issues found in the previous model. Section 4 presents the proposed multi-keyed model. In Section 5, the evaluation results are presented and discussed. Finally, the conclusion and the future work are presented in Section 6.

II. LITERATURE REVIEW

Following is a brief description of the previous works on securing the access control and RFID systems:

Malik et al. have focused on the access control on the cloud they focused on handling the situations at the time of requirement engineering by proposing a self-adaptive, risk-based access control framework by monitoring and estimate the user risk score and environmental factors continuously and reconfigure the system automatically by adjusting it to the changes happened to the system. Their framework was able to adjust to unprecedented changes also, based on the environmental factors, it can revoke the users to access the system and it may give the access to previously unauthorized users [11].

Tounsi et al. have added a driven privacy policy that is extracted from the contextual concepts from the extended Role Based Access Control model. They also forge the security rules by using the temporary concepts. They tested their model by using the Fosstrak platform, and they evaluate the performance of the model based in the execution time [12].

Dorri Nogoorani and Jalili have proposed the first trust-driven risk-aware access control framework, which complements access control services by monitoring the users and reduce the risk using obligations. In their proposed framework, they added to the Grid access control services the

risk management and trust evaluation, thus the user's responsibilities will be explicitly specified by the using of the obligations with the access control. Moreover, they mitigate risks by specifying specific obligations policies according to their severities. They have studied their framework on the European Grid Infrastructure (EGI), and they evaluate the performance of their framework and prove it is scalable by simulation using the JAVA language [13].

Mohandes et al. have attempted to control the types of the vehicles that access the Makkah at the Pilgrimage seasons by proposing a hybrid system for vehicle access control, which consists of automatic license plate recognition (ALPR) technologies and RFID technology. RFID is used to track the vehicles and localize them; they enhanced the RFID technology by adding the ALPR to it. This is happening by giving the authorized vehicles a passive RFID tag and specifying the schedule allowed to them before the Pilgrimage season. Additionally, the system will specify unauthorized vehicles by the ALPR technology. The system was tested over two Pilgrimage seasons and the results show that the system is able to recognize the vehicle when their speed is up to100km/h also the RFID accuracy was 100% and the ALPR was 94% [14].

Majumdar et al. have proposed a proxy agent framework to enhance the privacy of the users who is carrying the RFID tags by increasing the protection against cloning, eavesdropping and impersonation attacks. The proxy agent will help the user to decide which information to be released from the tag. Furthermore, they guaranteed that only the authorized users could control their tags [15].

Yang et al. have enhanced the security protocols depending on hash functions to achieve the goals of two-way authentication, by proposing a security mechanism in a kind of authentication and communication that achieve the functions of the conditional Access Module (CAM), which is used when authenticating the nodes in the remote education system. They have analyzed the system and it showed that it was safe, reliable, applicable, strong compatibility and applicable [16].

Fall et al. attempted to make the authorization algorithm more flexible by proposing the Risk Adaptive Authorization Mechanism (RAdAM) for cloud computing. In RAdAM, they had enhanced their mechanism by enforcing the decision using the vulnerability score of the object by complementing the RAdAM mechanism with the Vulnerability-based authorization (VBAM) mechanism which is a using the variation of the Bell_Lapandula MultiLevel Security (MLS). They have proved the practicability of the RAdAM mechanism using the fuzzy inference system and proved the usefulness of the RAdAM using a use case featuring OpenStack [17].

Raj et al. have proposed Bus security and Attendance management for schoolchildren using RFID to track the student's movements. In their proposed system they assume that each student will has a RFID tag and this tag will be read whenever the student enters or exits the bus, the bus database will be provided to the school admin database. In addition, they assume to add a reader in the classroom entrance in which each time the student enters or exits the classroom it will be notified. The student's attendance database will be allowed to her parents. They did not make any performance evaluation of their proposed system [18].

III. Security Issues in the Previous Models

This section highlights the main security issues with the identification and authentication process in the previously proposed models [19], [20], [4]. A new model for providing an enhanced security level for the identification and the authentication process in [4] is then proposed, evaluated and discussed in Section 4.

In [19], the authors proposed RFID access control system without using backend database. The system relies only on the RF subsystem for both identification and authentication without a backend database, often referred to as the serverless model. For this to happen, the RFID tag is used as a memory dump to store the access control information (e.g. name, headshot image, biometric features, access level, etc.) in an encrypted format. A symmetric cipher algorithm (i.e. Advanced Encryption Standard (AES)) is used to encrypt the access control information and the key is stored on a tamper-resistant memory chip inside each RFID reader in the system.

While the aforementioned design ensures high availability with minimum complexity and low implementation cost, it suffers from several issues in access management, users' permissions and system scalability, which were highlighted and addressed in [20].

A multi-module risk adaptive hybrid RFID access control system was proposed in [20]. The proposed system alternates between the serverless and server-based mode for authentication, authorization and access control decision-making based on the risk level, which is calculated dynamically using multiple risk factors in addition to a proposed risk calculation algorithm. The system utilizes a similar identification and authentication algorithm to the one that was proposed in [19] with minor modifications to accommodate the server-based mode. However, both systems are still relying on a symmetric cipher algorithm with a single key module to provide the confidentiality requirement.

In [4], A Multilevel Fuzzy Inference System (MFIS) was introduced to replace the "Risk Engine" module in the aforementioned system. The proposed MFIS has significantly improved the risk calculation process and has corrected some cases where the risk value was incorrectly estimated (over or under estimated). Additionally, the overall system performance was enhanced.

Nonetheless, relying on a single key symmetric encryption system places a great risk (both financially and security) in case this key or one of the RFID readers were to be compromised, which will affect the entire system.

IV. Enhanced Multi-keyed Proposed System

In this section, the issue of using a single encryption key in the previous models is addressed and a multi-keyed model is proposed to enhance the security of the identification and authentication process.

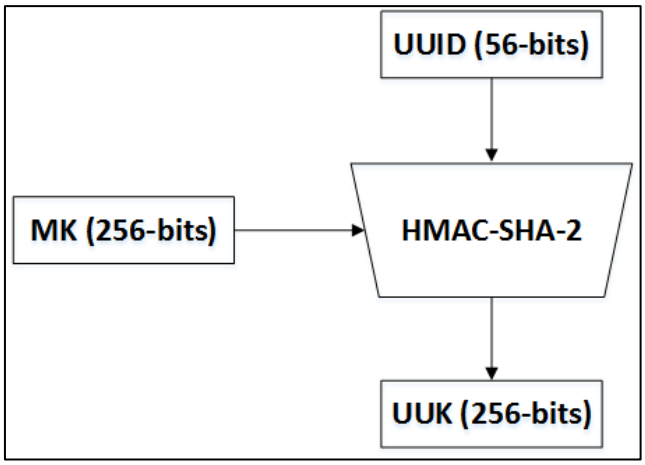

Fig. 1. Proposed User Symmetric Key Generation Model.

```
## benchmarker:          release 4.0.1 (for python)
## python version:       3.6.0
## python compiler:      MSC v.1900 64 bit (AMD64)
## python platform:      [redacted]
## python executable:    C:\Python36\python.exe
## cpu model:            Intel64 Family 6 Model 42 Stepping 7, GenuineIntel
## parameters:           loop=1000, cycle=1, extra=0

##                                 real    (total    = user    + sys)
Generate UUK                     0.0120    0.0000    0.0000    0.0000
Encrypt/Decrypt using UUK        0.1761    0.1719    0.1250    0.0469
Encrypt/Decrypt using MK         0.0510    0.0469    0.0469    0.0000

## Ranking                         real
Generate UUK                     0.0120  (100.0) ********************
Encrypt/Decrypt using MK         0.0510  ( 23.5) *****
Encrypt/Decrypt using UUK        0.1761  (  6.8) *

## Matrix                          real    [01]    [02]    [03]
[01] Generate UUK                0.0120   100.0   425.0  1466.7
[02] Encrypt/Decrypt using MK    0.0510    23.5   100.0   345.1
[03] Encrypt/Decrypt using UUK   0.1761     6.8    29.0   100.0
```

Fig. 2. Benchmark Evaluation for the Proposed Model.

Although relying on a symmetric encryption algorithm allow the system to operate significantly faster than asymmetric, it creates an issue in which the master key becomes a single point of failure that could compromise the security of the whole system in case its confidentiality, integrity or availability were to be compromised. In order to overcome this issue, the authors propose a multi-keyed model where each user has a unique symmetric key based on their User Unique Identifier (UUID).

In order to generate a symmetric encryption key for each user uniquely and on the fly without producing abundant modifications on the previously proposed identification and authentication model, the authors proposed using a keyed-Hash Message Authentication Code (HMAC). The UUID is fed to the HMAC function as data while the same Master Key (MK) used in the previous models for encrypting the access data is fed to the HMAC function as the secret cryptographic key. This approach guarantees that each user will have his/her unique key generated on the fly without the need to store it on the RFID reader; thus, preserving the same model while enhancing the security.

Assuming two inputs to the HMAC function, that is, 7-bytes UUID and 256-bits secret cryptographic key size, the output length need to be compatible with AES key size (128-bits, 196-bits or 256-bits). Using HMAC function based on Secure Hash Algorithm 2 (SHA-2), i.e. HMAC-SHA-2, will ensure meeting this requirement. In Fig. 1, the proposed model is presented, where the output is the User Unique Key (UUK).

As opposed to the previous models, MK is used to generate the UUK rather than encrypting the access control data stored on the access card. This will require re-encrypting the data using UUK.

The proposed model reserves the same data structure, in addition to the same identification and authentication process but with minor variation, that is, using the UUK instead of MK in the encryption and decryption process.

However, the overall processing time is slightly increased since the symmetric key has to be generated on the fly instead of reading it directly. The overall processing time becomes the total of; data transfer time + UUK generation time + decryption time + integrity checking time + decision-making time.

Using 7 bytes UUID gives the proposed model a high scalability where 2^{56} unique keys can be generated, which is hard to be encountered in most applications.

V. Results and Discussion

In this section, the proposed method is evaluated and the results are discussed then compared with the previous model.

In order to evaluate the proposed model, a simulation code was used to provide near estimate results of the effect that the proposed user symmetric key generation model might have on the overall processing time. The overall processing time is the total of; data transfer time, decryption time, verification time and decision-making time. The proposed model will have an effect on the decryption time only, leaving the others unchanged.

The simulation code is written in Python 3.6.0 and run on an Intel 64-bits PC with a 2.2 GHz CPU. The source-code[1] is provided for those who want to replicate the results.

A benchmark was performed in order to measure the effect of the newly proposed model and the result is shown in Fig 2. The benchmark is set to run for 1000 rounds and measures the main 3 functions (i.e. generate UUK, decrypt with UUK and decrypt with MK). The encryption function was not taken into consideration since in real-life systems it would be performed once when the access card is issued and never used again; thus, it is safe to ignore its value from the overall processing time. The results show that the time requirements for the proposed model is quite insignificant when compared with the other two functions. It also shows that when the generate UUK function is used in the verification process instead of reading the value of the MK directly, the system becomes subject to minimum degradation in the overall process.

[1] https://github.com/*********

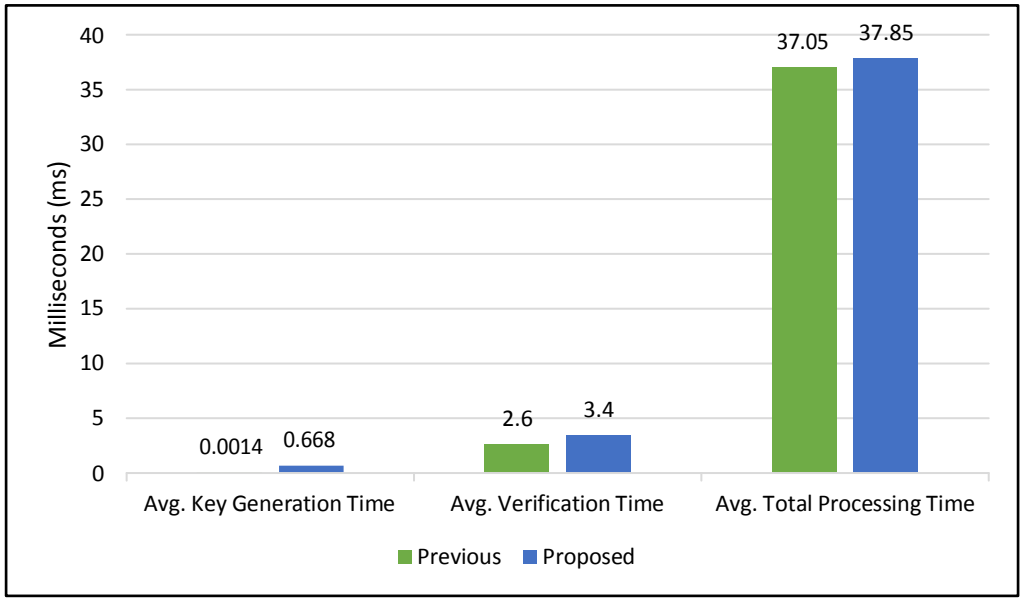

Fig. 3. Comparsion between the Processing Time of the Proposed Model vs. the Previous Model.

In order to calculate the difference between using the newly proposed method and the previous method, the average overall processing time was calculated for the two methods as shown in Fig 3. The experiment was executed 100 times on the same data and the average results indicates that the new method has imposed an insignificant delay of 0.8 milliseconds, which is the cost for generating the encryption key on the fly on average.

It is worth mentioning that the key generation time for the previous model is the time to read the master key (MK) from the memory. However, in the proposed model, it is the time to generate the UUK from the UUID and MK using the method described in Fig 1.

The imposed delay while insignificant, it provides an increased level of security, since:

- Each RIFD card is now being encrypted with its unique key.
- The encryption key itself is not stored on the RFID reader.
- Assuming the UUID is randomly generated and is not related to the user's information, then it is quite hard for an attacker to deduce for example user 2 UUK from user 1 UUK even if the master key is known.

The aforementioned benefits constitute great justification to support the use of the proposed model even though that it introduces minor delay to the overall processing time.

VI. Conclusion

Access control represents the first line of defense in the security arsenal that can make or break the security of any system. Traditional access control methods lacks the ability to adapt to the changing conditions. Risk adaptive/aware access control systems can solve this problem. In this paper, the authors continued to enhance on the previous model where a Risk Adaptive Hybrid RFID Access Control System with Multilevel Fuzzy Inference Controller was proposed, through adjusting the identification and authentication process by introducing a multi-keyed model to generate the symmetric encryption key dynamically on the fly instead of using the same key for all users. The result showed that the proposed model has increased the security of the system; however, introduced insignificant delay to the overall process time (i.e. milliseconds).

References

[1] A. Ahmed and N. Zhang, "Towards the realisation of context-risk-aware access control in pervasive computing," *Telecommun Syst*, vol. 45, no. 2–3, pp. 127–137, Dec. 2009.

[2] R. A. Shaikh, K. Adi, L. Logrippo, and S. Mankovski, "Risk-based decision method for access control systems," in *2011 Ninth Annual International Conference on Privacy, Security and Trust (PST)*, 2011, pp. 189–192.

[3] P. H. Cole and D. C. Ranasinghe, *Networked RFID Systems and Lightweight Cryptography: Raising Barriers to Product Counterfeiting*. Springer, 2008.

[4] M. Al-Zewairi, D. Suleiman, and A. Shaout, "Multilevel Fuzzy Inference System for Risk Adaptive Hybrid RFID Access Control System," in *2016 Cybersecurity and Cyberforensics Conference (CCC)*, 2016, pp. 1–7.

[5] K. Z. Bijon, R. Krishnan, and R. Sandhu, "A Framework for Risk-Aware Role Based Access Control," presented at the 2013 IEEE Conference on Communications and Network Security (CNS), National Harbor, MD, USA, 2013, pp. 462–469.

[6] P. C. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner, and A. S. Reninger, "Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control," in *2007 IEEE Symposium on Security and Privacy (SP '07)*, 2007, pp. 222–230.

[7] R. Doskočil, "An Evaluation of Total Project Risk Based on Fuzzy Logic," *Verslas: teorija ir praktika*, vol. 15, no. 2, pp. 23–31, Dec. 2015.

[8] Hany Sallam, "Cyber Security Risk Assessment Using Multi Fuzzy Inference System," *IJEIT*, vol. 4, no. 8, pp. 13–19, Feb. 2015.

[9] J. Li, Y. Bai, and N. Zaman, "A Fuzzy Modeling Approach for Risk-Based Access Control in eHealth Cloud," in *2013 12th IEEE*

International Conference on Trust, Security and Privacy in Computing and Communications, 2013, pp. 17–23.

[10] Q. Ni, E. Bertino, and J. Lobo, "Risk-based Access Control Systems Built on Fuzzy Inferences," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, New York, NY, USA, 2010, pp. 250–260.

[11] A. A. Malik, H. Anwar, and M. A. Shibli, "Self-adaptive access control delegation in cloud computing," in *2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 2016, pp. 169–176.

[12] W. Tounsi, N. Cuppens-Boulahia, F. Cuppens, and G. Pujolle, "Access and privacy control enforcement in RFID middleware systems: Proposal and implementation on the fosstrak platform," *World Wide Web*, vol. 19, no. 1, pp. 41–68, Jan. 2016.

[13] S. D. Nogoorani and R. Jalili, "TIRIAC: A trust-driven risk-aware access control framework for Grid environments," *Future Generation Computer Systems*, vol. 55, pp. 238–254, Feb. 2016.

[14] M. Mohandes, M. Deriche, H. Ahmadi, M. Kousa, and A. Balghonaim, "An Intelligent System for Vehicle Access Control using RFID and ALPR Technologies," *Arab J Sci Eng*, vol. 41, no. 9, pp. 3521–3530, Sep. 2016.

[15] S. Majumdar, K. Dhuri, S. S. Dongre, and M. R. Badwaik, "RFID Tag Security, Personal Privacy Protocols and Privacy Model," *International Journal of Exploring Emerging Trends in Engineering (IJEETE)*, vol. 3, no. 04, pp. 247–251, 2016.

[16] L. Yang, Q. Wu, Y. Bai, H. Zheng, and S. Lin, "An improved hash-based RFID two-way security authentication protocol and application in remote education," *Journal of Intelligent & Fuzzy Systems*, vol. 31, no. 5, pp. 2713–2720, Oct. 2016.

[17] D. Fall, T. Okuda, Y. Kadobayashi, and S. Yamaguchi, "Risk Adaptive Authorization Mechanism (RAdAM) for Cloud Computing," *Journal of Information Processing*, vol. 24, no. 2, pp. 371–380, 2016.

[18] M. Raj, S. Pote, A. Mhaske, and R. Mahakale, "Bus Security And Attendance Management For School Children Using RFID," *Imperial Journal of Interdisciplinary Research*, vol. 2, no. 3, Feb. 2016.

[19] M. Al-Zewairi, J. Alqatawna, and O. Al-Kadi, "Privacy and Security for RFID Access Control Systems: RFID Access Control Systems without back-end database," presented at the 2011 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), Amman, Jordan, 2011, pp. 272–277.

[20] M. Al-Zewairi, J. 'far Alqatawna, and J. Atoum, "Risk adaptive hybrid RFID access control system," *Security Comm. Networks*, vol. 8, no. 18, pp. 3826–3835, Dec. 2015.