A new Model of Multi-Key Generation for RFID Access Control System

Mustafa Al-Fayoumi[1], Malek Al-Zewairi[1, 2], and Salam Hamdan[1]
[1]Computer Science Department, Princess Sumaya University for Technology, Jordan
[2]Jordan Information Security and Digital Forensics Research Group

Abstract: *When studying traditional access control models, one could conclude that they have been proven inefficient in handling modern security threats, with access decisions influenced by several factors, including situational, environmental and risk factors. Accordingly, several studies have proposed risk-aware access control models to overcome the limitations of the traditional models. In this paper, the authors continue to improve on a previously proposed risk adaptive hybrid access control system, in which risk assessment is performed using a multilevel fuzzy inference system, by introducing an enhanced multi-key model for generating the symmetric encryption key dynamically for each user on demand. Consequently, the proposed model helps in solving the issue of having a single point of failure caused by employing a master encryption key, as in the previous models. The experimental results show that the proposed multi-key model does, indeed, improve the overall security of the system while preserving the previous model architecture and with negligible processing overhead.*

Keywords: *Encryption key generation model, Risk-based access control, Radio frequency identification.*

Received February 10, 2018; accepted April 17, 2018

1. Introduction

Access control is an essential countermeasure to protect against unauthorized access attempts and to enforce permissions and security settings in a system. Several models for access control have been proposed and discussed in the literature over the years including Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC) and many others [17].

Previously, access control models relied on predefined rules to grant and revoke permissions; such models are referred to as traditional access control models. Although these models provide a simple means of managing access control, they suffer from an inability to adapt to changing conditions imposed by dynamic environments where there is a constant need to grant or revoke access permissions based on multiple factors, whether temporal, environmental, situational or operational [3].

Conversely, in risk-based access control models, permissions are assigned, revoked, increased or decreased based on the risk level of the requested operations, thus making them more suitable for dynamic environments [1, 3, 26].

Radio Frequency Identification (RFID) is a prominent wireless technology for short-range communications. The RFID technology has been widely adopted in access control applications due to its wireless nature, small form, ability to perform cryptographic functions and other calculations, low cost, and the fact that, in most cases, it does not require an internal power source (e.g., passive RFID tags) [2, 4, 9, 18,19, 21, 24, 28, 29].

While adopting a risk-based approach for access control offers great advantages over traditional models, measuring the risk value qualitatively is often subject to over- or under-estimation, making the system prone to error. Alternatively, fuzzy logic has proved effective in applications where uncertainty significantly affects the outcomes of the system. Consequently, several Fuzzy Inference Systems (FISs) have been proposed in the literature as part of risk-based access control models [4, 6, 7, 12, 22, 25].

In this paper, the authors continue to enhance the previously proposed RFID access control systems [2, 3, 4]. These systems utilize symmetric cryptographic algorithms to provide confidentiality and integrity for the access information in the system. Nonetheless, a master secret key is used to encrypt the access information for all users, making it a single point of failure in case its confidentiality, integrity, or availability were to be compromised. Therefore, a multi-key model for generating the symmetric encryption key dynamically for each user is proposed and evaluated. Accordingly, a compromised RFID tag or reader will not affect the entire system, unlike in the previous models.

The rest of this paper is organized as follows. In section 2, recent research efforts on access control systems are discussed. Section 3 highlights the security issues found in the previous models. Section 4 then explains the proposed multi-key model. In section 5, the evaluation results are presented and discussed. Finally, the conclusion and future work are presented in section 6.

2. Literature Review

The following is a brief discussion of the recent research efforts on access control systems.

Malik *et al.* [20] focused on cloud access control at the time of requirement engineering by proposing a self-adaptive risk-based access control framework. Their proposed framework continuously monitors and estimates the user risk score in addition to the environmental factors, and then reconfigures the system automatically to adjust to the changes.

Tounsi *et al.* [28] added a driven privacy policy that is extracted from the contextual concepts from the extended RBAC model. Additionally, the security rules were forged using the temporary concepts. The model was tested using the Fosstrak platform and was evaluated based on its execution time.

Nogoorani and Jalili [23] proposed the first trust-driven risk-aware access control framework, which complements access control services by monitoring the users' activities and reduces the risk using obligations. In their proposed framework, they added to the Grid access control services the risk management and trust evaluation; thus, the users' responsibilities will be explicitly specified by using obligations with access control. Moreover, they mitigated risks by specifying specific obligations policies according to their severities. Furthermore, they evaluated their framework on the European Grid Infrastructure (EGI) and proved its scalability using custom simulation application written in Java.

Mohandes *et al.* [21] attempted to control the types of vehicles that access Makkah City during the Pilgrimage season. They proposed a hybrid system for vehicle access control, which consists of Automatic Licence Plate Recognition (ALPR) technologies and passive RFID tags. The proposed system recognizes authorized vehicles via passive RFID tags, ALPR and a specified schedule. The system was tested over two Pilgrimage seasons and the results show that it was able to recognize vehicles when their speeds were less than 100km/h. The RFID accuracy was 100%, while the ALPR accuracy was 94%.

Majumdar *et al.* [19] proposed a proxy agent framework to enhance the privacy of the users carrying RFID tags by increasing the protection against cloning, eavesdropping and impersonation attacks. The proxy agent allows the user to control which information is to be released from the tag.

Yang *et al.* [29] proposed an enhanced security protocol to provide mutual authentication between the RFID reader and the tag. The proposed protocol relies on sending a hashed value of the RFID tag unique ID concatenated with a nonce to the reader instead of sending the actual ID. Then, a backend system recursively tries to match the hashed value with a tag ID in its database. If successful, a hashed value of the tag ID and a new nonce is sent to the tag, thus achieving mutual authentication. Moreover, formal analysis of the proposed protocol was provided and compared with three protocols.

Fall *et al.* [13] proposed a Risk Adaptive Authorization Mechanism (RAdAM) for cloud computing that utilizes a real-time vulnerability-based authorization mechanism based on the Bell–LaPadula model. Interestingly, RAdAM employs a two-variable FIS (i.e., object sensitivity and subject clearance) to calculate the risk score using a Gaussian membership function.

Huh *et al.* [15] proposed an access control framework for distributed access control systems in wired and wireless networks, which assures that access policies are guaranteed while maintaining the least-privilege principle. The proposed framework was presented by a model architecture that is appropriate to the industrial control system community.

Shu *et al.* [27] took advantage of sensory information to achieve the dynamic authentication in access control systems, which is different from the previous access control systems that rely on the static information stored on the access card. In their paper, they introduced two case studies and theoretically analysed the increasing of the key size. They also conducted a performance evaluation by building a prototype of the proposed system. Thereafter, they validated the mechanism of the authentication experimentally. The results showed an accuracy of 95% between different users, which is considered high.

Ferdous *et al.* [14] attempted to reveal the violations of policy in distributed access control systems by proposing a blockchain-based decentralized monitoring infrastructure for Distributed access system (DRAMS). The authors claim that the proposed infrastructure has no single point of failure and that it guarantees the integrity and the availability of the stored logs.

Kardas *et al.* [16] provided a security analysis of two chaotic map-based authentication protocols, which were found to be vulnerable to tag owner tractability, RFID tag cloning and desynchronization attacks. They also proposed a Chebyshev chaotic map-based authentication protocol to overcome the aforementioned attacks.

Dass and Om [10] proposed a secure server-based authentication protocol for RFID systems in which they utilized two pseudorandom number generators (PRNG) (one used by the reader and the other by the tag), one-way hash function and XOR operation.

The proposed protocol provided mutual authentication between the RFID tag and reader in a way that is secure against most common attacks (e.g., replay, desynchronization, MitM, DoS, and traceability). In addition, it offered desirable security features such as tag anonymity, forward secrecy, confidentiality and integrity. However, Chikouche [8] disproved their claims and showed that the proposed protocol failed to provide secure authentication in addition to the tag intractability feature.

Lv *et al.* [18] analysed three of their previously proposed RFID authentication protocols that utilize elliptic curve cryptography (ECC) and showed that they are vulnerable to tag tractability attacks. They then proposed an enhanced protocol that is supposed to be resistant to tag tractability attacks.

However, An *et al.* [5] showed that the proposed protocols are also vulnerable to MitM attacks and proposed three new ECC-based protocols to overcome these vulnerabilities.

Dinarvand and Barati [11] proposed an ECC-based RFID authentication protocol to provide mutual authentication between the RFID tag and the reader. The protocol was then compared with four recent protocols in terms of security features, performance, computational cost, communication cost, and storage requirements.

3. Security Analysis of the Previous Models

In this section, the authors provide a security analysis of the previously proposed models [2, 3, 4].

Al-Zewairi *et al.* [2] proposed a serverless RFID access control model that relies solely on the radio frequency subsystem of an RFID system to perform both the identification and the authentication functions, without using any backend system. In order to abandon the traditional server-based model, the RFID tag is treated as a memory dump to store the encrypted access control information (e.g., name, headshot image, biometric features, access level, etc.,), which allows the model to refrain from using backend database. A symmetric cipher algorithm, the advanced encryption standard (AES), is used to encrypt the access control information. Moreover, the secret key is stored on a tamper-resistant memory chip inside each RFID reader in the system, and thus, is never sent over the air.

Although the aforementioned design ensures high availability with minimum complexity and low implementation cost, it suffers from several issues, including the lack of access management and low scalability, which were subsequently highlighted and addressed [3].

Additionally, Al-Zewairi *et al.* [3] introduced a multi-module risk adaptive hybrid RFID access control model that alternates between serverless and server-based modes for identification, authentication and authorization functions based on the risk level of the requested operation. The proposed model operates, by default, in the serverless mode as long as the risk level is under a certain threshold; otherwise, it switches to the server-based mode in order to enforce stricter security controls or change the access permissions. As with the previous model, the new model still relies on a symmetric cipher algorithm with a single secret key to provide the confidentiality requirement. Nevertheless, it significantly improves the overall security of the system due to the tight integration of risk in the decision-making process, the higher scalability and the reintroduction of access management with the server-based mode.

A Multilevel Fuzzy Inference System (MFIS) with two levels and four fuzzy variables was proposed [4] to replace the “Risk Engine” module in the aforementioned model. The proposed MFIS significantly improved the risk calculation process by addressing the uncertainty issue using fuzzy logic instead of binary logic. Moreover, it corrected some cases where the risk value was incorrectly estimated (over- or under-estimated). Consequently, the new model employs considerably fewer rules to calculate the risk value under the same risk scenarios (from 200 to 73 rules), thus significantly improving the overall system performance. Nonetheless, as with the previous models, it still relies on a single key symmetric encryption system, which creates a significant risk, both from a security point of view and financially, if this key were to be compromised, hence affecting the entire system.

Admittedly, the three models share the same weakness imposed by the usage of one key to encrypt the access information for all users, having a single point of failure that if compromised, would affect the whole system.

4. Enhanced Multi-Key Model

In this section, the issue of using a single encryption key in the previous models is addressed and a multi-key model that dynamically generates a unique encryption key for each user when the RFID tag is presented at the reader is proposed. This multi-key model is integrated with the MFIS proposed by Al-Zewairi *et al.* [4].

Although relying on a symmetric encryption algorithm allows the system to operate significantly faster than with an asymmetric algorithm, it creates an issue in which the master key becomes a single point of failure that could compromise the security of the whole system if its confidentiality, integrity or availability were to be compromised. In order to overcome this issue, the authors propose a multi-key model in which each user has a unique symmetric key generated based on their User Unique Identifier (UUID). In the proposed model, the UUID is considered a randomly generated value that can be used to identify any user in the system uniquely. Nonetheless, the UUID might also be any other value that uniquely identifies the user, such as their employee/student ID or social security number.

In order to generate a symmetric encryption key for each user uniquely and dynamically without producing abundant modifications on the previously proposed model, the authors propose using a keyed-Hash Message Authentication Code (HMAC) function to generate the keys dynamically when the RFID tag is presented at the reader. 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 a unique key generated dynamically when needed without the need to store it on the RFID reader nor the tag, thus preserving the same model architecture while enhancing the overall security.

Assuming the two inputs to the HMAC function, that is, the 7-byte UUID and the 256-bit secret cryptographic key, the output length needs to be compatible with AES key size (128-bits, 196-bits or 256-bits). Using the HMAC function based on the secure hash Algorithm 2 (SHA-2), i.e. HMAC-SHA-2, ensures that this requirement is met. In Figure 1, the proposed model is presented, where the output is the User Unique Key (UUK). Using the 7-byte UUID gives the proposed model a high scalability where 2^{56} (72,057,594,037,927,936) unique keys can be generated, which is rarely encountered in most access control applications. Moreover, the proposed model preserves the same data structure, in addition to the same identification and authentication process, but with a minor variation, namely, the usage of UUK instead of MK in the encryption and decryption process.

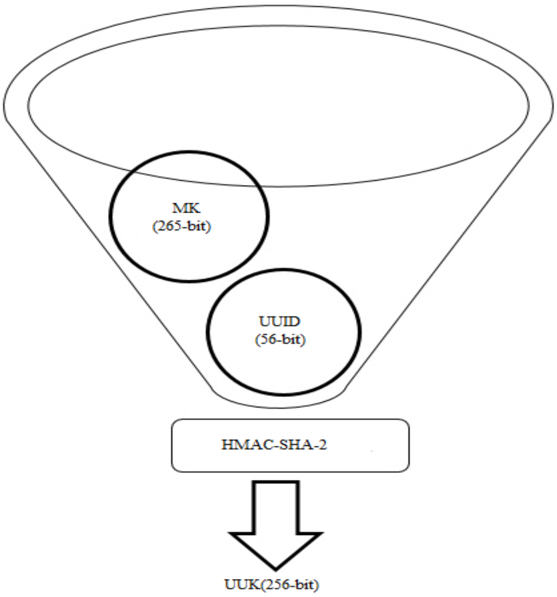


Figure 1. Proposed Symmetric Key Generation Model.

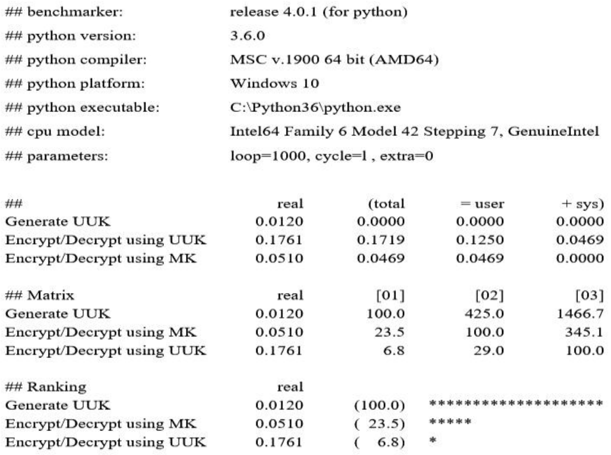
Unlike in the previous models, MK is used to generate the UUK rather than encrypting the access control data stored on the access card. This will require re-encrypting the data using UUK. However, the overall processing time is slightly increased since the symmetric key has to be generated on the fly instead of reading it directly from a tamper-resistant memory. The overall processing time becomes the sum of data transfer time, UUK generation time, decryption time, integrity checking time and decision-making time.

5. Results and Discussion

In this section, the proposed multi-key model is evaluated and the results are discussed and then compared with those of the previous model.

In order to evaluate the proposed model, a simulation code is used to provide near estimate results of the effect that the proposed multi-key model might have on the overall processing time. As mentioned in Section 4, the overall processing time is the sum of data transfer time, UUK generation time, decryption time, integrity checking time and decision-making time. However, only the UUK generation time is newly introduced. 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 executed on an Intel 64-bit PC with a 2.2 GHz CPU. The source-code[1] is provided for those interested in replicating the results.

Furthermore, a benchmark is performed in order to measure the effect of the proposed multi-key model, and the results are shown in Figure 2. The benchmark is set to run for 1000 rounds and measures the three main functions, namely, generate UUK, decrypt with UUK and decrypt with MK. The encryption function is 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 exclude its value from the overall processing time. Moreover, the data transfer time constitutes a variable that is affected by many factors, such as the tag type, the reader type, the number of tags in the reader vicinity and the distance between the tag and the reader; hence, it can also be safely ignored.



```
## benchmarker:              release 4.0.1 (for python)
## python version:           3.6.0
## python compiler:          MSC v.1900 64 bit (AMD64)
## python platform:          Windows 10
## python executable:        C:\Python36\python.exe
## cpu model:                Intel64 Family 6 Model 42 Stepping 7, GenuineIntel
## parameters:               loop=1000, cycle=l , 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

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

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

Figure 2. Benchmark Evaluation for the Proposed Model.

[1] https://github.com/alzewairi/Multikey_MFIS_RFID

The results show that the overhead introduced by the proposed model is quite insignificant when compared with the other two functions. Moreover, when the “generate UUK” function is used in the integrity verification process instead of reading the value of the MK directly, the system becomes subject to minimum degradation in the overall process time.

In order to calculate the difference between using the proposed multi-key model and the previous method, the average overall processing time is calculated for the two methods, as shown in Figure 3.

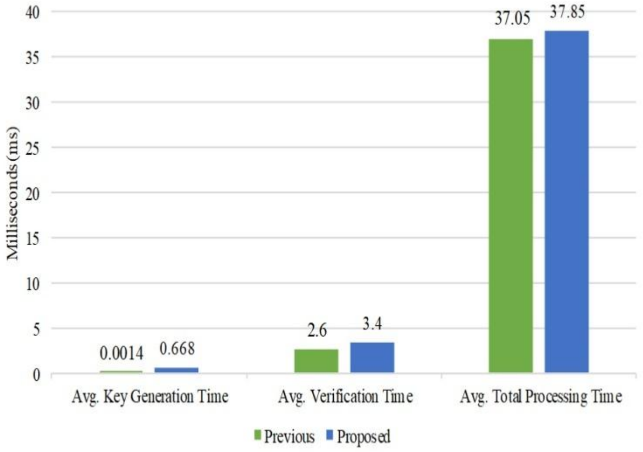


Figure 3. Comparison between the Processing Time of the Proposed Multi-Key Model and the Previous Model.

The experiment is executed 100 times on the same data, and the average results indicate that the proposed model has imposed an insignificant delay of 0.82 milliseconds, which is the cost of generating the encryption key dynamically 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 tamper-resistant memory. However, in the proposed model, it is the time needed to generate the UUK from the UUID and MK using the method described in Figure 1.

The imposed delay, in addition to being insignificant, provides an increased level of security, since:

- Each RFID tag is encrypted with its unique key; thus, if one tag is compromised, the other tags are not affected, unlike in the previous models.
- The encryption key itself is not stored on the RFID reader but generated dynamically when needed.
- Assuming the UUID is randomly generated and is not related to the user’s information, it is quite difficult for an attacker to deduce the key for one tag from another tag.

The aforementioned benefits constitute substantial justification for supporting the use of the proposed model, even though it introduces a minor increase in the overall processing time.

6. Conclusions

Access control represents the first line of defence in the security arsenal that can make or break the security of any system. However, traditional access control models lack the ability to adapt to the changing conditions imposed by modern dynamic environments. Risk-aware access control models are receiving attention within the research community as an alternative way to overcome the limitations of traditional models.

In this paper, the authors enhanced on the previous model where a risk adaptive hybrid RFID access control system with a multilevel fuzzy inference controller was proposed, by introducing a multi-key model to generate the symmetric encryption key dynamically on demand instead of using the same key for all users. The results showed that the proposed model significantly improves the security of the system, while introducing a negligible increase (i.e., 0.82 milliseconds) in the overall process time.

References

[1] Ahmed A. and Zhang N., “Towards the Realisation of Context-Risk-Aware Access Control in Pervasive Computing,” *Telecommunication Systems*, vol. 45, no. 2-3, pp. 127-137, 2009.

[2] Al-Zewairi M., Alqatawna J., and Al-Kadi O., “Privacy and Security for RFID Access Control Systems: RFID Access Control Systems without Back-End Database,” *in Proceedings of the IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies*, Amman, pp. 272-277, 2011.

[3] Al-Zewairi M., Alqatawna J., and Atoum J., “Risk Adaptive Hybrid RFID Access Control System,” *Security Communication Networks*, vol. 8, no. 18, pp. 3826-3835, 2015.

[4] Al-Zewairi M., Suleiman D., and Shaout A., “Multilevel Fuzzy Inference System for Risk Adaptive Hybrid RFID Access Control System,” *in Proceedings of Cyber security and Cyber forensics Conference*, Amman, pp. 17, 2016.

[5] An R., Feng H., Liu Q., and Li L., “Three Elliptic Curve Cryptography-Based RFID Authentication Protocols for Internet of Things,” *in Advances on Broad-Band Wireless Computing, Communication and Applications*, 2016.

[6] Bijon K., Krishnan R., and Sandhu R., “A Framework for Risk-Aware Role Based Access Control,” *in Proceedings of IEEE Conference on Communications and Network Security*, National Harbor, pp. 462-469, 2013.

[7] Cheng P., Rohatgi P., Keser C., Karger P., Wagner G., and Reninger A., “Fuzzy Multi-

Level Security: An Experiment on Quantified Risk-Adaptive Access Control," *in Proceedings of IEEE Symposium on Security and Privacy*, pp. 222-230, 2007.

[8] Chikouche N., "Formal Analysis of a Novel RFID Authentication Protocol," *in Proceedings of the 8th International Conference on Computing, Communication and Networking Technologies*, pp. 1-7, 2017.

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

[10] Dass P. and Om H., "A Secure Authentication Scheme for RFID Systems," *Procedia Computer Science*, vol. 78, pp. 100-106, 2016.

[11] Dinarvand N. and Barati H., "An Efficient and Secure RFID Authentication Protocol Using Elliptic Curve Cryptography," *Wireless Networks*, pp. 1-14, 2017.

[12] Doskočil R., "An Evaluation of Total Project Risk Based on Fuzzy Logic," *Business: Theory and Practice*, vol. 17, no. 1, pp. 23-31, 2016.

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

[14] Ferdous M., Margheri A., Paci F., Yang M., and Sassone V., "Decentralised Runtime Monitoring for Access Control Systems in Cloud Federations," *in Proceedings of the IEEE 37th International Conference on Distributed Computing Systems*, pp. 2632-2633, 2017.

[15] Huh J., Bobba R., Markham T., Nicol D., Hull J., Chernoguzov A., Khurana H., Staggs K., and Huang J., "Next-Generation Access Control for Distributed Control Systems," *IEEE Internet Computing*, vol. 20, no. 5, pp. 28-37, 2016.

[16] Kardaş S. and Genç Z., "Security Attacks and Enhancements to Chaotic Map-Based RFID Authentication Protocols," *Wireless Personal Commu*nications, vol. 98, no. 1, pp. 1135-1154, 2018.

[17] Karp A., Haury H., and Davis M., "From ABAC to ZBAC: The Evolution of Access Control Models," Technical Report, 2009.

[18] Lv C., Li H., Ma J., and Zhang Y., "Vulnerability Analysis of Elliptic Curve Cryptography-Based RFID Authentication Protocols," *Transactions on Emerging Telecommunications Technologies*, vol. 23, no. 7, pp. 618-624, 2012.

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

[20] Malik A., Anwar H., and Shibli M., "Self-Adaptive Access Control Delegation in Cloud Computing," *in Proceedings of 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, Shanghai, pp. 169-176, 2016.

[21] Mohandes M., Deriche M., Ahmadi H., Kousa M., and Balghonaim A., "An Intelligent System for Vehicle Access Control using RFID and ALPR Technologies," *Arabian Journal for Science and Engineering*, vol. 41, no. 9, pp. 3521-3530, 2016.

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

[23] Nogoorani S. and Jalili R., "TIRIAC: A Trust-Driven Risk-Aware Access Control Framework for Grid Environments," *Future Generation Computer Systems*, vol. 55, pp. 238-254, 2016.

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

[25] Sallam H., "Cyber Security Risk Assessment Using Multi Fuzzy Inference System," *International Journal of Engineering and Innovative Technology*, vol. 4, no. 8, pp. 13-19, 2015.

[26] Shaikh R., Adi K., Logrippo L., and Mankovski S., "Risk-Based Decision Method for Access Control Systems*," in Proceedings of 9th Annual International Conference on Privacy, Security and Trust*, pp. 189-192, 2011.

[27] Shu Y., Gu Y. J., and Chen J., "Dynamic Authentication with Sensory Information for the Access Control Systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 427-436, 2014.

[28] Tounsi W., Cuppens-Boulahia N., Cuppens F., and Pujolle G., "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, 2016.

[29] Yang L., Wu Q., Bai Y., Zheng H., and Lin S., "An Improved Hash-Based RFID Two-Way Security Authentication Protocol And Application in Remote Education," *Journal of Intelligent and Fuzzy Systems*, vol. 31, no. 5, pp. 2713-2720, 2016.

Mustafa Al-Fayoumi received a BSc degree in Computer Science from Yarmouk University, Irbid, Jordan, in 1988. He earned an MSc degree in Computer Science from the University of Jordan, Amman, Jordan, in 2003, and his PhD in Computer Science from the Faculty of Science and Technology at Anglia University, UK, in 2009. Currently, he is the Dean's Assistant for King Hussein School of computing sciences at Princess Sumaya University for Technology (PSUT), Jordan. His research interests include computer security, cryptography, identification and authentication, wireless and mobile networks security, e-application security, simulation and modelling, algorithm analyses and design, information retrieval, data mining and other related topics.

Malek Al-Zewairi is an Information Security Researcher, Consultant, and Trainer. He has over six years of experience in the information security field and holds more than 16 Professional Security Certificates. He also sits on several International Security Boards and Committees. Malek is currently, a PhD candidate at Princess Sumaya University for Technology studying Computer Science with a focus on information security. His research interests lie primarily in the area of intelligence and security informatics, network security and RFID.

Salam Hamdan is a PhD candidate in Computer Science at Princess Sumaya University for Technology. She received her bachelor's degree in Computer Engineering from Al-Balqa Applied University, 2012. She received her master's degree in Information System Security and Digital Criminology from Princess Sumaya University for Technology (PSUT), 2015. Her research interests include hardware security, network security and vehicular ad hoc networks.