SELMS: A Secure E-Library Management System

Mohammed Issam Younis Ph.D (Asst.Prof.)* Mustafa Hashim Abdulkareem*

Abstract

The RFID technology stands at the forefront of the technologies driving the Internet of Things (IoT) and Internet of Everything (IoE) vision. However, using RFID technology has bleeding edges in adopting it for sensitive applications because RFID still has security and privacy issues. This paper reviews the state-of-the-art of RFID and security issues and proposes an enhancement for three-pass authentication protocol based on passive RFID and cryptographic services (i.e., digital signature and password-based encryption schemes) to make the adoption of such sensitive applications more practical. As a proof of concept, this paper proposes a secure E-library management system (SELMS) and gives the architectural and detailed design of the system modules in terms of Unified Modeling Language (UML) diagrams to facilitate the implementation of such system in a real environment.

Keywords: IoT, IoE, RFID, Authentication Protocol, Encryption, Digital Signature, UML.

* Baghdad University

1. Introduction

The Internet of Things (IoT) refers to a broad technological vision enabling a completely new concept of living called “intelligent life”. Smart devices, smartphones, smart cars, smart homes, smart cities, smart transport, smart energy, smart industry, smart world are synonyms that describe new paradigm in the world of Internet. IoT enables affluence of new opportunities different from the traditional one [1]. IoT is not a single standalone technology, it is a system of technologies which can monitor the status of physical objects, capture meaningful data, and communicate that data over a network to a software application for analysis on a dedicated computer or to the cloud. Objects can be electronic devices such as a utility meter, organisms or a natural part of the environment such as an area of ground to be measured for moisture or chemical content. A smart device is associated with each object which provides the connectivity and a unique digital identity for identifying, tracking and communicating with the object. A sensor within or attached to the device is connected to the Internet by a local area connection (such as Radio Frequency Identification (RFID), Near Field Communication (NFC) or Bluetooth Low Energy (BTLE)) and can also have wide area connectivity. Typically, each data transmission from a device is small in size but the number of transmissions can be frequent. Each sensor will monitor a specific condition or set of conditions such as vibration, motion, temperature, pressure or utility quality. More applications have become feasible because the cost and size of such devices continue to decrease and their sophistication for measuring conditions keeps increasing. Technological giant Cisco predicts that by 2020, there will be over 50 billion permanently connected “things”, with over 200 billion with intermittent connections [1].

The term "Internet of Things" was used for the first time by Kevin Ashton at MIT Auto-ID center in 1999. In its early stage, IoT used RFID tags, and thereafter, the concept has changed little by little up to the point of the current ubiquitous computing environment. By 2020, it is expected that physical world web service also will be included [2]. Terms that have similar meanings with IoT include Machine-to-Machine (M2M), Wireless Sensor Network (WSN)/ Ubiquitous Sensor Network (USN), Internet of Everything (IoE) [2].

Technologies suitable for IoT which exist today are short range (RFID) and WSN, plus few more in development. RFID together with NFC and Wireless Sensor and Actuator Networks (WSAN) are recognized as “the atomic components that will link the real world with the digital world”. In current literature, the RFID is presented as a technology which can implement the IoT vision because of low cost and strong existing support from business community [1]. So, RFID technology can have a

significant impact in this regard since it is now mature to provide part of the IoT device layer (physical layer) of the IoT architecture [3]. RFID technology is one of the emerging technologies that is being used by organizations such as manufacturers, retailers, logistics providers, hospitals, and libraries [4]. RFID is a new generation of Auto Identification and Data collection technology which helps to automate business processes and allows identification of a large number of tagged objects like books, using radio frequency (RF) waves [5]. As shown in Figure 1, an RFID system is comprised of a tag (transponder), a reader (interrogator), and a host computer (software application) [6]. The tag which is the key component of RFID contains unique ID number of the item to which it is attached [4]. RFID tags consist of an etched antenna and a microchip, which stores data including a unique ID number to identify each item. RFID tags can be either active – having their own battery power source, or passive – having no power source of its own so passive tags draw power from the electromagnetic waves emitted through the air by the reader and use it to power the microchip's circuits [7]. RFID Readers are units that usually placed in certain places to recognize the transponders [6]. Readers consist of a transmitter, receiver, and antenna. They communicate with RFID tags, identify them and retrieve and write the information on RFID tags [7]. The reader sends tag's information to a host computer through its control lines to complete the whole information processing [8]. However, RFID system has security challenging issues due to its highlights computation. Motivated by such challenge, this paper proposes a secure M2M security protocol to be integrated into an RFID-based library system called a secure E-library management system (SELMS). This paper is organized as follows. Section 2 highlight some related works in adopting RFID in the library system, and discusses the security issues in RFID systems. Section 3 proposes an enhancement for a three-pass authentication protocol. Section 4 gives the architectural and detailed design of the SELMS. Finally, Section 5 states the conclusion and gives some suggestion for future work.

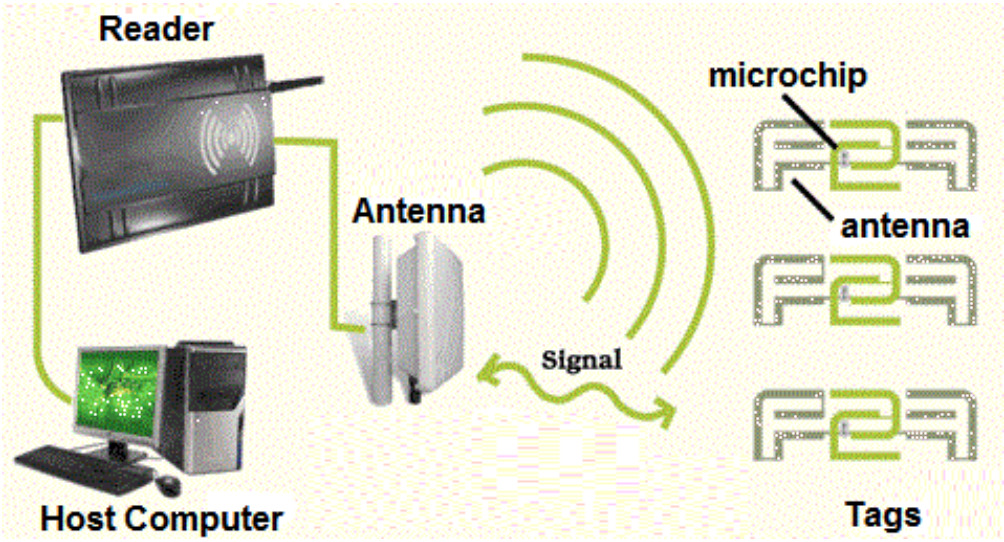

Figure 1 RFID System.

2. Related Works

This section reviews the adopting of the RIFD in library systems in the literature, and highlight the security problems in RFID systems and the cryptographic schemes to facilitate problem solution.

2.1. RFID in Libraries

Like as the business sector, libraries have been using RFID technology since the late 1990s. Hundreds of libraries in Malaysia, UK and US and other countries have implemented RFID and the vast majority of these libraries are positive about their RFID investment and its benefits. Since traditional systems were proved to be less effective, RFID has become a solution in time. According to the reports of the implementation, it was seen that the libraries which used RFID technology made their tracking, identifying and controlling system more efficient [4]. The main motive of using RFID technology in libraries is to decrease the time consumption of every task, to minimize the manual intervention, and to eliminate manual errors. The RFID facilitates the fast issuing, reissuing and returning of books with the help of RFID-enabled modules. It directly provides the book information and library member information to the library management system and does not need the manual typing. It also provides monitoring and searching system [5]. RFID system doesn't require to have so much money to be set up in libraries since one library could set up RFID system with approximately $20.000-30.000. After this cost, the system did not require any high-cost equipment of other things to keep going. Only tag cost could exist and the cost of tags was about 0.22 cent which is a negligible amount for businesses. In

addition, when RFID system works in the library, the management doesn't need to have many personnel in the library since the library uses radio waves to identify books and library members automatically so, the libraries could have RFID technology with a conceivable cost to provide both time and staff savings. With the usage of the portable handheld reader, the library could finish all kind of operations such as counting inventory, scanning books, finding books, borrowing and returning books in a short time [4]. Circulation includes check-out, check-in, and renewal of the documents. It usually takes 1-2 min to complete a single transaction when the task is performed manually, while the same transaction takes place within 1-2 s with the RFID system [7]. As such, integrating RFID into library management system makes both the library users and staff's task easy, smart, convenient and practical [6].

2.2. Security Issues with RFID Technology

It's become clear that RFID technology offers many benefits in libraries but every technology has its problems [8]. Security and privacy of RFID are very questionable since major problems come from wireless communications which are vulnerable to various attacks. RFID systems need to be designed and implemented with adequate security and privacy protection [1]. RFID is a wireless technology and therefore it is subject to third-party interception unless the signal is secured. There is a perception among some that RFID is a threat to privacy since RFID tags may contain sensitive information and that they can be read by third-party [7]. As so, people believe that their privacy has been violated, which is one of the biggest problems that restrict the technology's development. RFID data security means protecting the data on the tag and the data transmitted between the tag and the reader to ensure it is accurate and safe from unauthorized access. RFID tag can be read from its range distance and its' contents can be read by anyone with an appropriately equipped scanner (RFID reader) [8]. This may cause two problems concerning data collection. On the one hand, usually, RFID tags in library systems are passive and reply to readers queries regardless of the desire of their proprietary. Thereby, individuals' data could be collected without them even knowing about it. On the other hand, an attacker can eavesdrop the reply from a tag to another authorized reader to impersonate that tag. In addition, Data integrity solutions are required in an RFID system to ensure that an adversary cannot modify data in the tag or during the data exchanging without detecting the change by the system. RFID tags are spread over a wide area and spend most of the time unattended. Data can be modified by adversaries while it is stored in the RFID tag or when it traverses the network [9]. Although a number of light-weighted RFID authentication protocols have been

developed for security and privacy protection in [10-17], but they all have serious problems and can't solve the security and privacy problems described above [18-25]. So, a reliable and heavy-weighted security protection mechanism for RFID is still in demand to solve the above-mentioned security and privacy issues.

2.2.1. RFID Authentication Protocol

In this section, the "Mifare Classic" tags with their three-pass mutual authentication protocol [26] is used since these tags are widespread and their cost is cheap and their protocol is scalable i.e. it does not use a database to authenticate both RFID reader and tag so the authentication time to an item is same as billion items. But similar to other RFID authentication protocols, this protocol has serious problems [27, 28] and can't solve the security problems; namely: privacy protection, impersonation, and data integrity.

2.2.2. Digital Signature Scheme

The conventional handwritten signatures on documents are used to certify that the signers are responsible for the documents' content. The signatures are physically part of the documents. It is difficult to do so convincingly, while the forgery is certainly possible. Thus, there is a need to have a way to sign the documents digitally which is functionally equivalent to a physical signature, but which is at least as resistant to forgery as its physical counterpart. The algorithms that can provide the functionality described above are called the Digital Signature Algorithms (DSAs). An DSA has two components, a private signing algorithm which permits a user to sign a document securely and a public verification algorithm which permits anyone to verify the signature [29]. DSAs were proposed in August 1991 by the U.S. National Institute of Standards and Technology (NIST) and was specified in a U.S. government federal information processing standard called the Digital Signature Standard (DSS) [30].

DSAs can be used to provide the following basic cryptographic services:
1- Data integrity: the assurance that data has not been altered by unauthorized or unknown means.
2- Data origin authentication: the assurance that the source of data is as claimed.
3- Non-repudiation: the assurance that an entity cannot deny previous actions or commitments [30].

The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve (EC) analogue of DSAs. ECDSA was first proposed in 1992 in the response to NIST request for public comments on their proposal for Digital Signature Schemes [29]. It was accepted in 1999 as an ANSI standard and was accepted in 2000 as IEEE and NIST standards and it was also accepted in 1998 as an ISO standard and is under

consideration for inclusion in some other ISO standards [30]. ECDSAs are recommended to be used in digital signatures because the strength-per-key-bit is substantially greater in EC systems than in other conventional systems. Thus, smaller parameters that are used in EC Cryptosystem than with digital logarithm systems but with equivalent levels of security. The advantages that can be gained from this feature include faster computations and smaller keys and certificates [29]. Thus, ECDSA has a smaller key size, which leads to faster computation time and reduction in processing power, storage space, and bandwidth. This makes the ECDSA ideal for constrained devices such as RFID tags [30].

In general, ECDSAs consist of three phases, the phase of key generation, phase of signing and phase of verifying. The key generation phase generates a key pair for each signer. Each key pair is consisting of a private key and a related public key. The signer maintains the secrecy of the private key which is employed for signing documents. In addition, the signer makes authentic copies of the public key which are employed to verify signatures. In the signing phase, a signer uses his private key to sign documents. And in the phase of verifying, a verifier uses the public key of the signer to verify the digital signature. The signer and verifier can be servers (computers) which perform necessary operations (i.e., key pair generation, signing documents, and verifying signatures). The signing phase includes two necessary steps to obtain the signatures. First, a signer uses a one-way hash function to calculate a hash value (h) of the data (d). The second step is generating the signature by encrypting “h” using the signer’s private key. The verifying phase includes three indispensable steps to notarize the signature’s validity. The first step is using Hash(d) to compute a certain hash value (h1) of the received “d”. The second step is calculating another hash value (h2) by decrypting the signature using the public key of the signer as shown in Figure 2. Finally, the third step is verifying the signature’s validity. If “h1” and “h2” are equal, the data (document) is authenticated and its integrity is maintained. The 256 bit is the recommended key length for EC cryptosystem [31]. Therefore, it is considered as the default key length value for ECDSA.

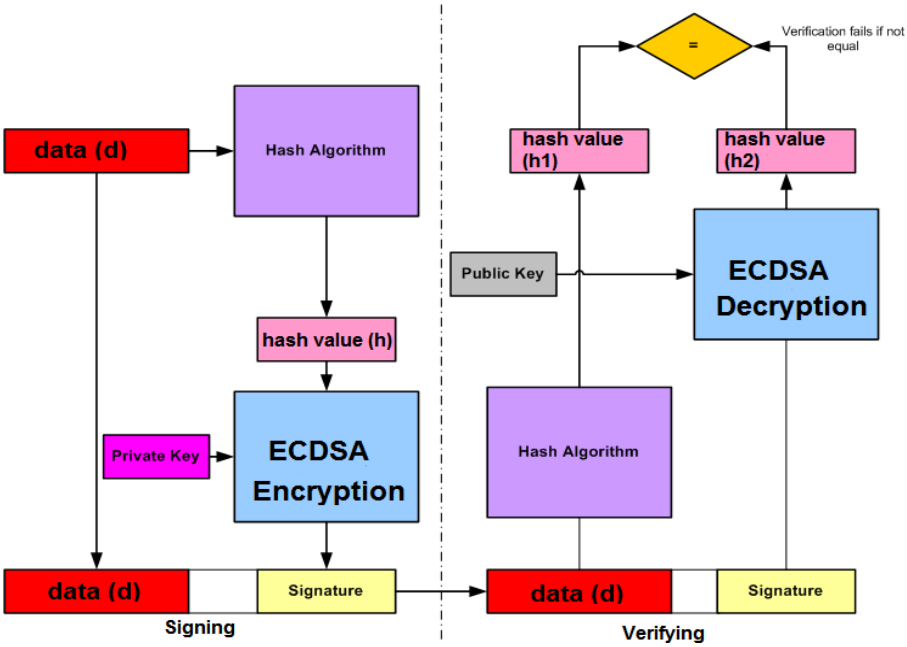

Figure 2 Signing and Verifying Phases of ECDSA.

2.2.3. Password Based Encryption Scheme

How to communicate securely over unsafe channels like radio frequency (RF) channels is a fundamental problem in cryptography. The unsafe channels may be controlled by an adversary. It is common in this scenario for two parties to encrypt and authenticate their messages in order to protect the privacy and authenticity of the exchanged data [32]. The sensitive information in unsafe channels needs to be encrypted to protect the privacy of this information in such channels. The sensitive information (e.g., the private key of digital signature) will be encrypted before storing it on RFID tags to provide privacy protection to that information. Some users want to encrypt and decrypt their sensitive information with an easy to remember the password (key) and at the same time be confident that their sensitive information is secure from prowling eyes. The loss or compromise of sensitive information is disastrous to the user. Password-based encryption (PBE) is designed to solve the problems described above. PBE algorithms are used to generate a secret key based on a password, which will be provided by the end user. Currently, there are two standards (PKCS #5 and #12) that define how a password can be used to generate a secret key. A good PBE algorithm will also mix in a random number called the salt along with the password to create the key. Without using the salts, the hackers can perform a brute force search for the key-space with relative ease [33].

In this paper, the advanced encryption standard (AES) PBE scheme is used to encrypt the sensitive information. The recommended key length for AES

cryptosystem is 256 bit [32]. Therefore, it is considered as the default key length value for AES PBE.

3. The Improved RFID Authentication Protocol

In this section, an improved mutual authentication protocol is proposed using the 256-bit AES PBE and 256-bit ECDSA to solve the security and privacy issues described in the previous section. The improved protocol consists of three phases as follows.

3.1. Authentication Phase

In this phase, the tag and the reader authenticate each other by carrying out the three-pass authentication protocol [26] as follows.

a. The RFID reader first requests to be authenticated for a particular sector of tag's memory.

b. The RFID tag generates a challenge nonce using a shared secret key and transmits the generated challenge nonce to the RFID reader and this is the first pass.

c. The reader calculates a response to tag's challenge and generates a challenge nonce using the shared secret key. Then, the reader sends the nonce and the reader response to the RFID tag and this is the second pass.

d. If the reader's response is correct, the RFID tag will respond with an answer and this is the third pass. If the reader response is incorrect, the tag will not respond and the communication is finished.

3.2. Data Writing and Password Setting Phase

In the case of writing data to the RFID tag, this phase is performed after the authentication phase. In this phase, the tag's owner must enter a password called "tag's password". This password is used to authenticate the tag's holder since only the genuine tag's owner knows the password. The tag's password is also used to derive an encryption key to encrypt the sensitive information of tag's owner including the password itself before writing it in the tag. If the information is not sensitive, the server writes that information as plaintext in the tag without encryption. But, if the information is sensitive, it will be encrypted by the server using the PBE to provide privacy protection. After encrypting the sensitive information including tag's password, the server signs the information using ECDSA private key before writing it on the RFID tag. The private and public keys of ECDSA are written in special tags called "signing and verification tags". Then, the server writes the information and

digital signature in the tag. Figure 3 shows the “Authentication” and “Data Writing and Password Setting” phases.

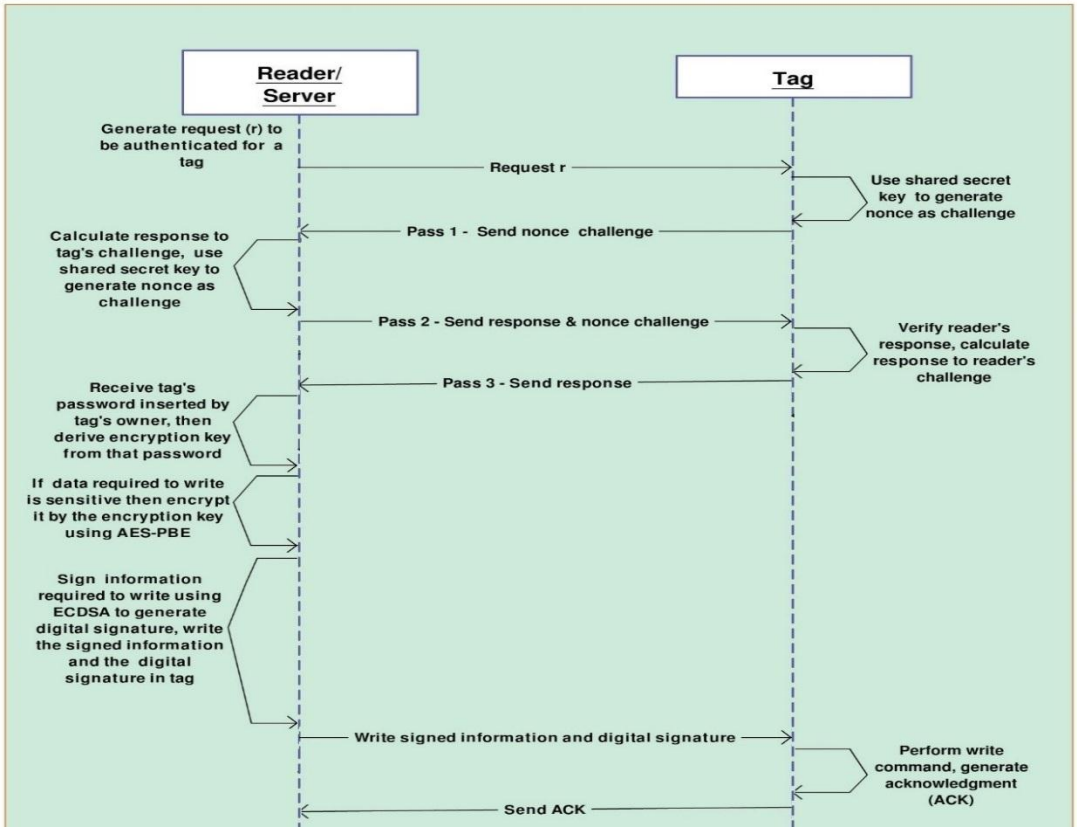

Figure 3 “Authentication” and “Data Writing and Password Setting” Phases of the Proposed Protocol.

3.3. Data Reading and Password Testing Phase

In the case of reading data from the tag, this phase is performed after the authentication phase. In this phase, the password test will be performed after reading the information stored in the tag by the server. The purpose of this test is to authenticate the tag’s holder by asking the tag’s holder to enter the tag’s password which is only known by the tag’s owner. Thereby, preventing tag impersonation. After inserting the password, the server derives the decryption key from that password and uses the key to decrypt the encrypted password and other sensitive information (if any) which are stored in the tag using AES PBE. Then, the server compares the inserted password with the decrypted password to verify the tag’s holder. After the verification, the server reads the digital signature from the tag and verifies the digital signature using ECDSA public key stored in the signing and verification tag. If the digital signature is verified, the tag’s owner is authenticated. Otherwise, he or she is

not authenticated and communication is finished. Figure 4 shows the “Authentication” and “Data Reading and Password Testing” phases.

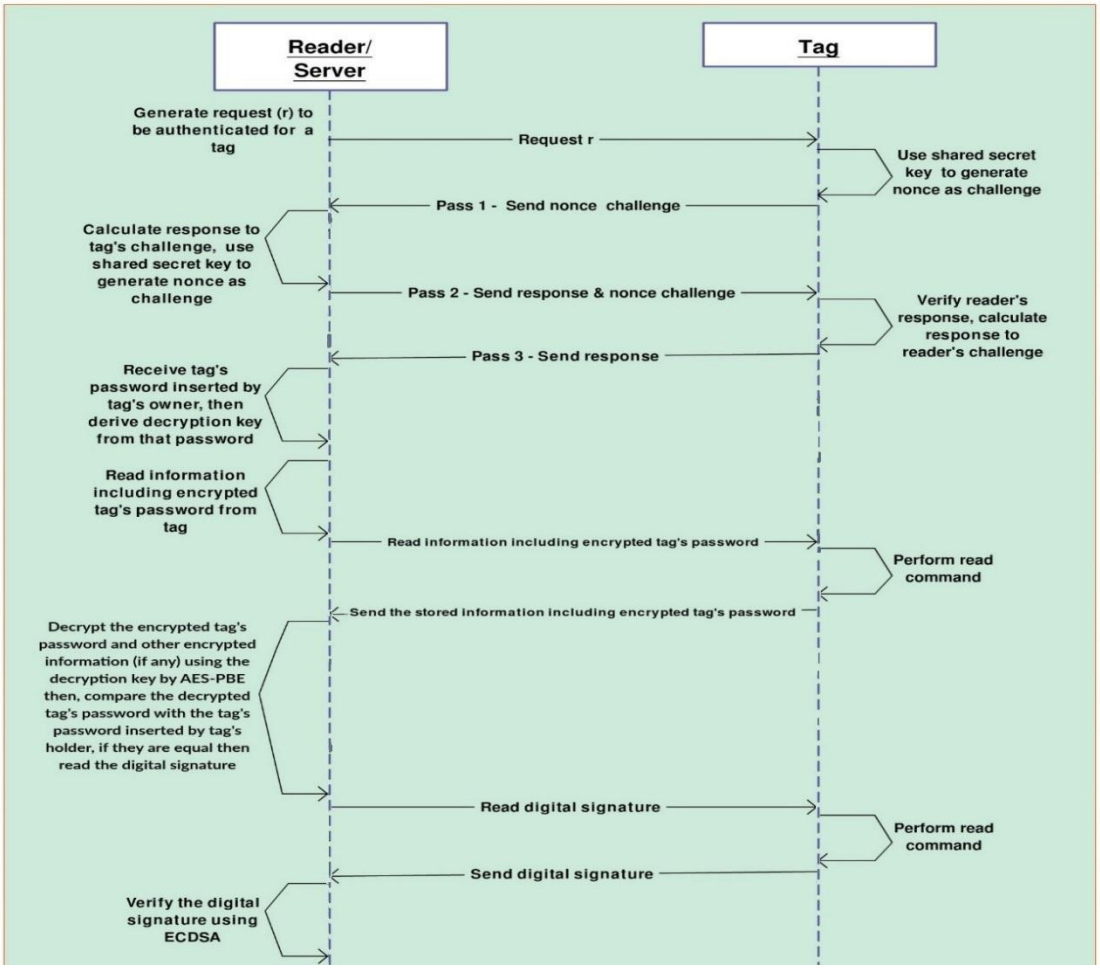

Figure 4 “Authentication” and “Data Reading and Password Testing” Phases of the Proposed Protocol.

4. The Proposed Secure E-Library Management System (SELMS)

This section proposes a secure e-library management system (SELMS) based on the proposed three-pass authentication protocol described in the previous section. SELMS modifies the design of SLMS [6] to make the system more secure. The SELMS consists of supervisor administrator, administrators, system users, library members, books, identification cards (tags), signing and verification cards (tags), identification devices (RFID readers, each reader attached to an antenna), anti-theft alarm, and server(s) (computers) contains the system’s modules and connected to a

database server that can be accessed through a web server, and a reliable network that is shared by all system's parts. In the SELMS, each system's administrator, user, and member has a unique identification (admin_id, user_id and member_id). This admin_id, user_id, and member_id are written on passive tags (admin_id, user_tag and member_tag). Similarly, for books, each book is attached with a passive tag (book_tag) so each book has a unique identification (book_id). The PC is connected to the RFID readers through a reliable network.

The system consists of six modules; namely: Initialization Module, Member Entry Module, Book Entry Module, Books Borrowing Module, Books Returning Module, and Books Monitoring Module.

4.1. Initialization Module

The initialization module is the first stage in the system's operation. It interacts with four actors, namely, the supervisor administrator and administrators on one side, and the administrators and users on the other side. According to functionality, the initialization module can be separated into two parts, the first of which is the creation of new administrators. In this part, the signing and verification tags of administrators (admin_tags) are created. With this part of the module, the supervisor administrator enters information related to a system's administrator(s) who will use the signing and verification tag(s) (admin_tags). This information includes the full name of the administrator, gender, mobile number and email. As shown in Figure 5, the supervisor administrator can create new administrators by simply providing the software with the required information.

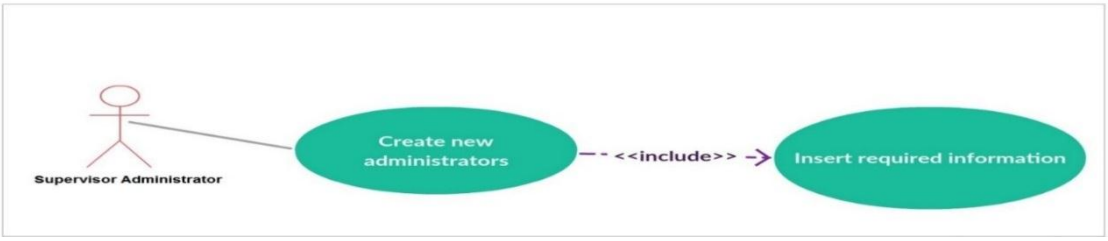

Figure 5 Use Case Diagram for the Creation of New Administrators (Interaction with Supervisor Administrator).

On the other hand, the server handles the generation of unique ECDSA key pair (private and public keys that are needed for the signing and verification functions) and the storage of administrator's information with ECDSA key pair into the signing and verification tag of the administrator (Figure 6).

Figure 6 Use Case Diagram for the Creation of New Administrators (Interaction with Server).

In order to complete the scenario described by the use cases, a sequence diagram in Figure 7 is constructed to show all the classes and messages needed for this module. The second part of the module has to do with creating new users. Just like in creating new administrators, all that is asked from the administrator to create new users is to insert the required information. Everything else is handled by the server as shown in Figures 8 and 9. The sequence diagram for the 'Creating New Users' module is demonstrated in Figure 10

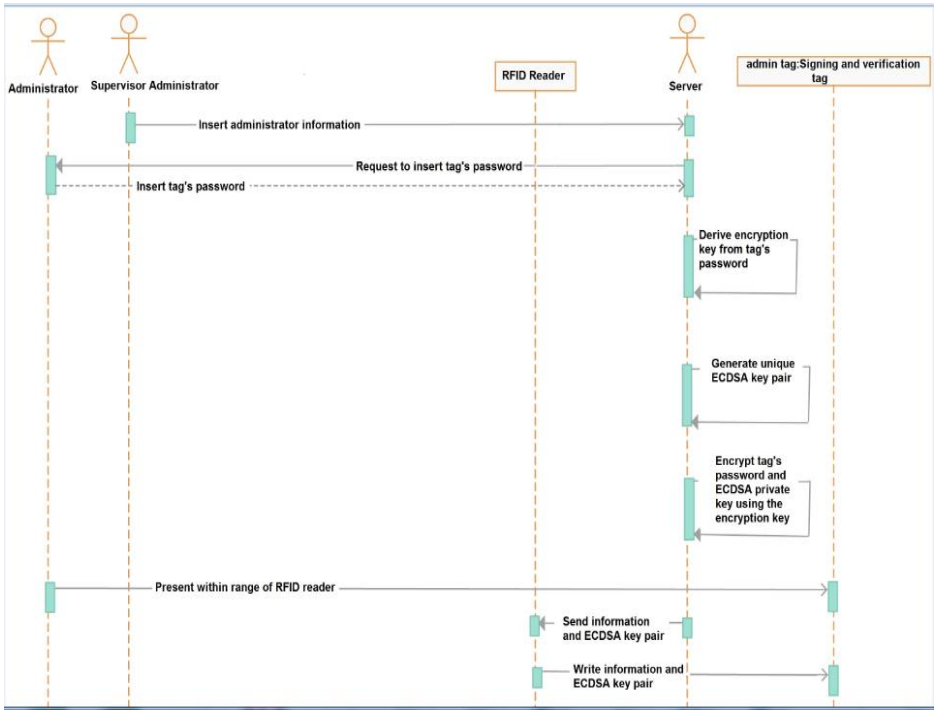

Figure 7 Sequence Diagram for Creating New Administrators.

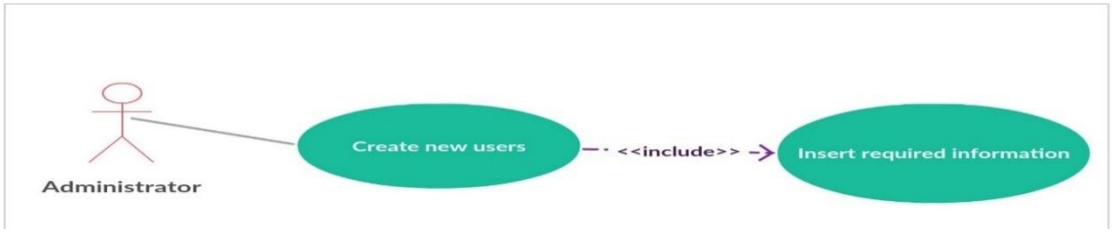

Figure 8 Use Case Diagram for Creating New Users (Interaction with Administrator).

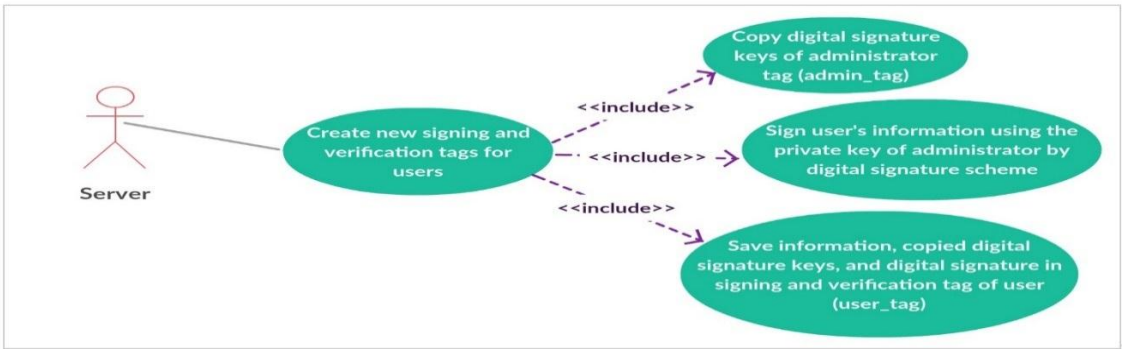

Figure 9 Use Case Diagram for Creating New Users (Interaction with Server).

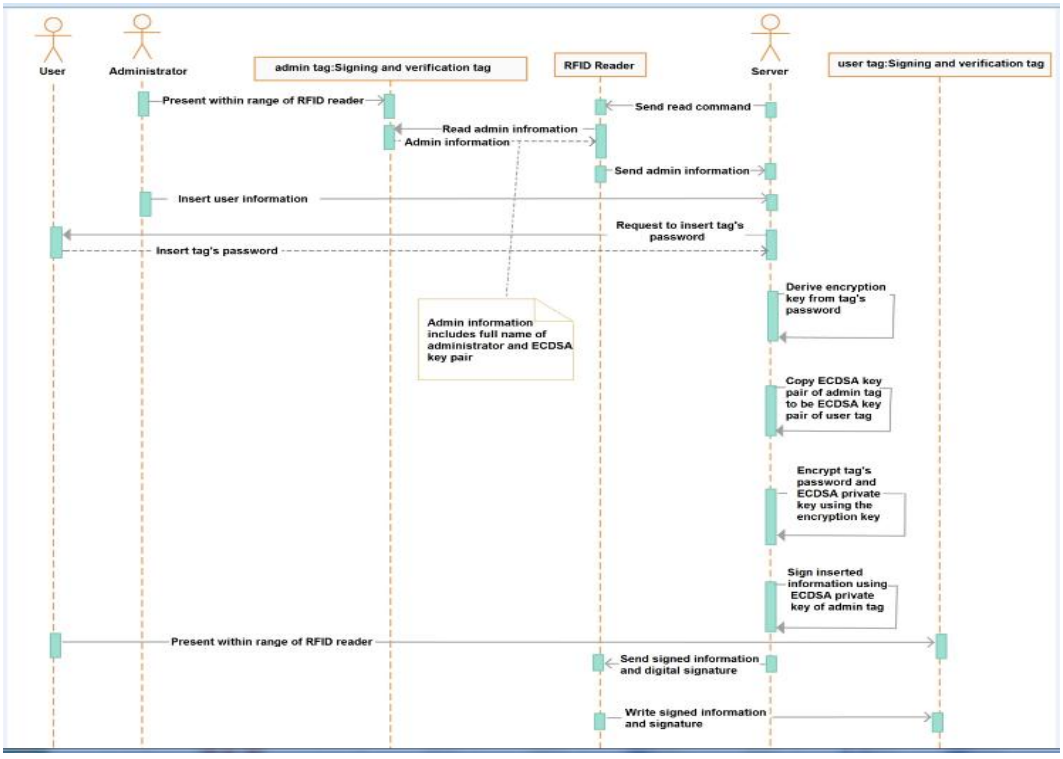

Figure 10 Sequence Diagram for Creating New Users.

4.2. Member Entry Module

The member entry module is used for inserting library member's information such as full name of the library member, the maximum period of borrowing, the maximum number of books allowed to be borrowed, the tag's password to authenticate the tag's holder, etc. Then the inserted information will be signed using the signing and verification tag of the user (user_tag), then the signed information will be saved with the digital signature in the member_tag. The use cases of the member entry module are shown in Figures 11 and 12.

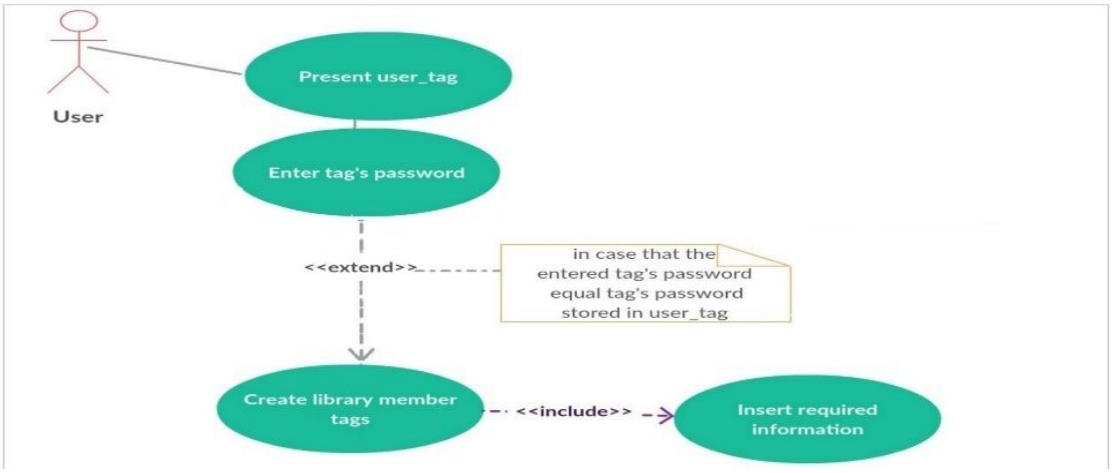

Figure 11 Use Case Diagram for Member Entry Module (Interaction with User).

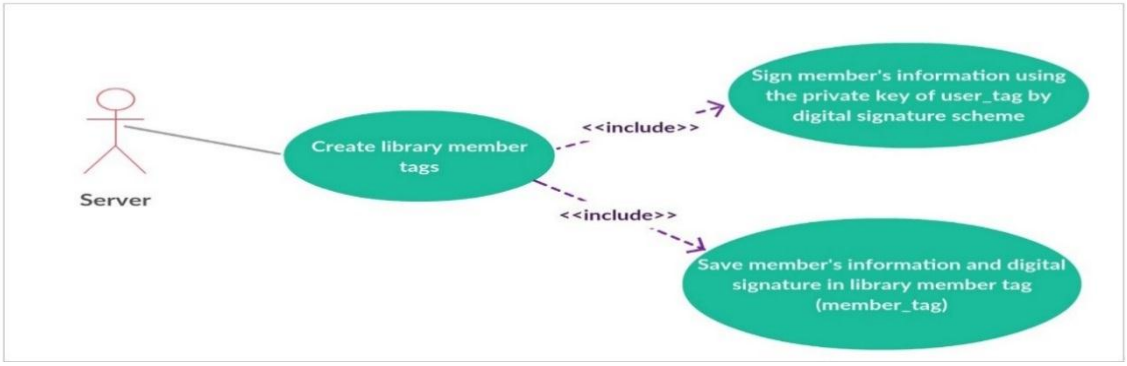

Figure 12 Use Case Diagram for Member Entry Module (Interaction with Server).

4.3. Book Entry Module

The book entry module is used for inserting the title of the book, a masking bit, and other information (author(s), publisher, year, request for borrowing by users, the location of the book, etc.). The purpose of the masking bit is to monitor whether the book inside the library and does not be borrowed (true) or outside the library (false, that is, the book is borrowed). Initially, the masking bit is activated (set to true). After inserting the required information, it will be signed using a signing and verification tag of system's user then, it will be saved with the digital signature in the book_tag. The use cases of the book borrowing module are shown in Figures 13 and 14.

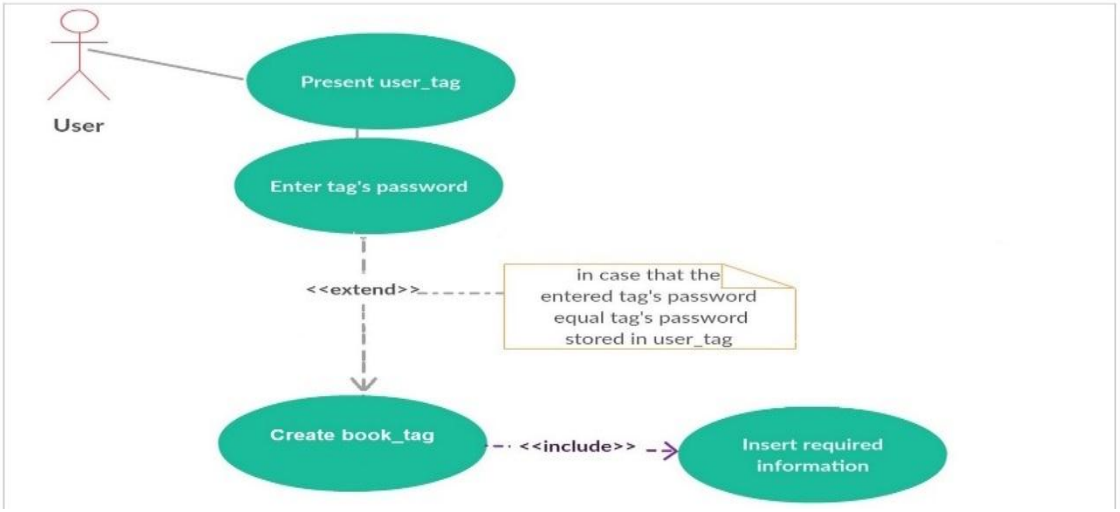

Figure 13 Use Case Diagram for Book Entry Module (Interaction with User).

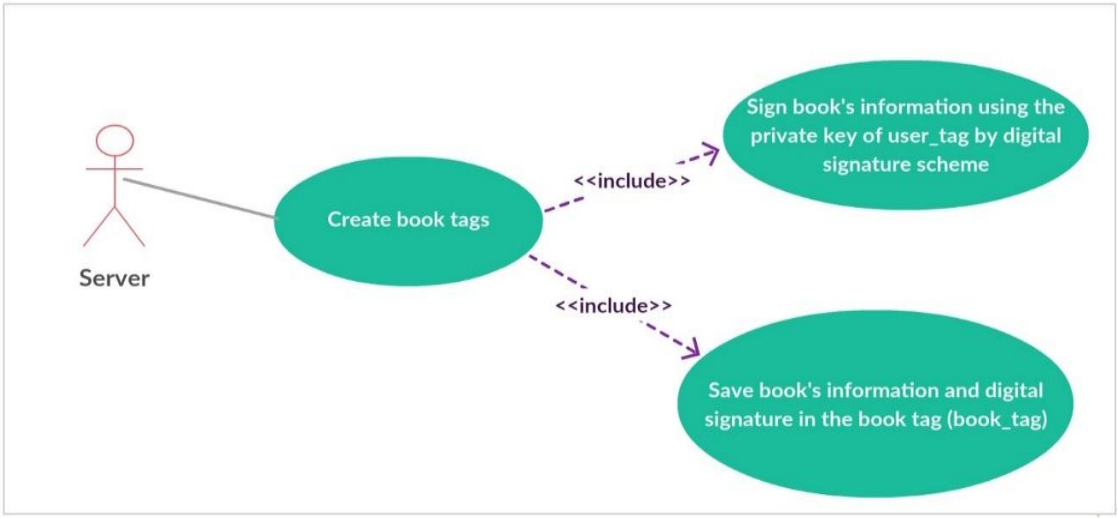

Figure 14 Use Case Diagram for Book Entry Module (Interaction with Server).

4.4. Books Borrowing Module

The books borrowing module is used by the library members for borrowing books operation. This module works as follows. When a library member presents his/her tag (member_tag), the server will identify the member_tag by verifying the digital signature in that tag using signing and verification tag of library user (user_tag) then it will ask the member to insert the tag's password to authenticate the tag's holder (the member). Next, the server asks the member to present the books then it receives the detected book_tags from RFID reader. After that, the server changes their status to be borrowed (by updating the masking bit for each book to be borrowed in the book_tags to false). The use case of the book borrowing module is shown in Figures 15 and 16.

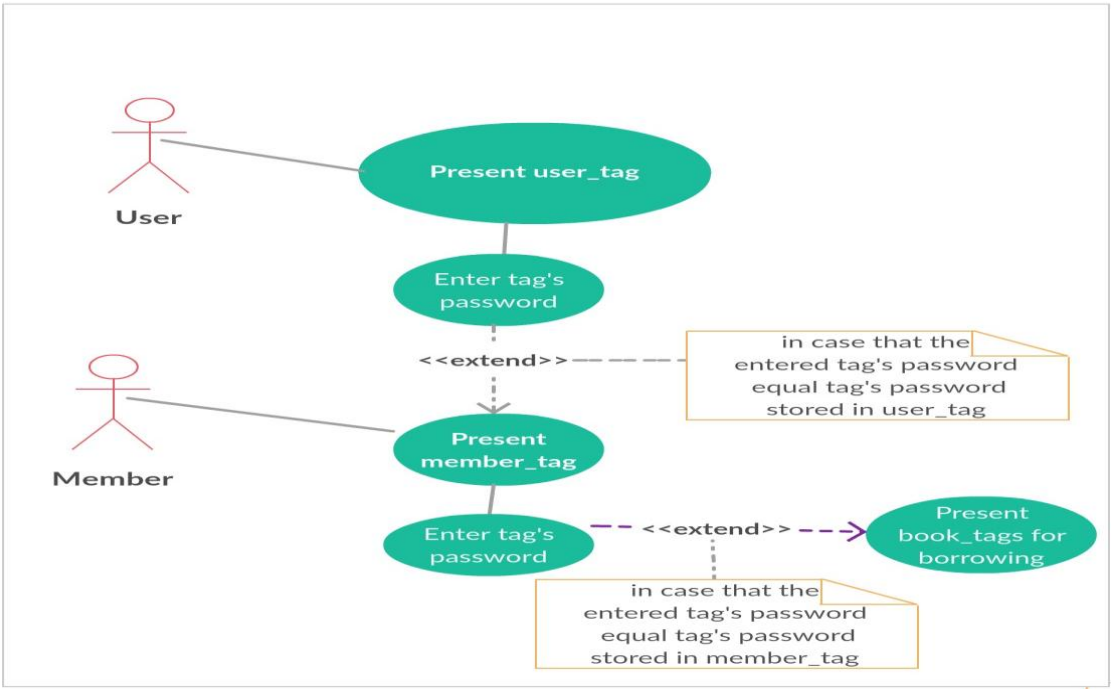

Figure 15 Use Case Diagram for Books Borrowing Module (Interaction with User and Member).

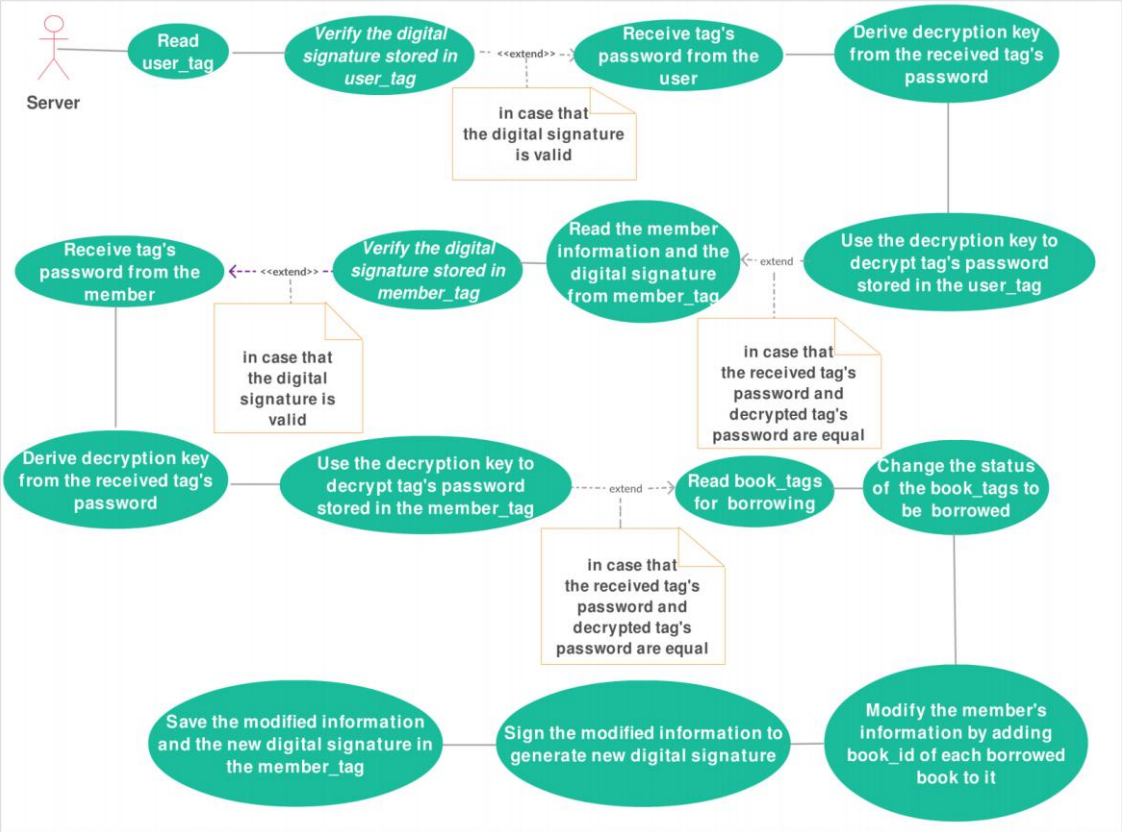

Figure 16 Use Case Diagram for Books Borrowing Module (Interaction with Server).

4.5. Books Returning Module

The books returning module is used by the library members for returning books operation. This module works as follows. When a member presents his/her tag (member_tag), the server identifies and verifies that tag using the signing and verification tag of system's user (user_tag) then it will ask the member to insert the tag's password to authenticate the tag's holder (the member). After that, the server will ask the member to present the borrowed books. Next, the server will receive the book_tags from RFID reader and verifies them by verifying the digital signature in book_tag of each book. After that, the server read the information in the book_tags to determine the borrowing period (whether or not the returning books within the allowed period). The server displays a GUI that issuing a penalty in a case that the maximum period of the allowed borrowing is exceeded. Finally, the server activates the masking bits (by updating the masking bit for each book to be returned in the book_tags as true). The use cases of this module are depicted in Figures 17 and 18.

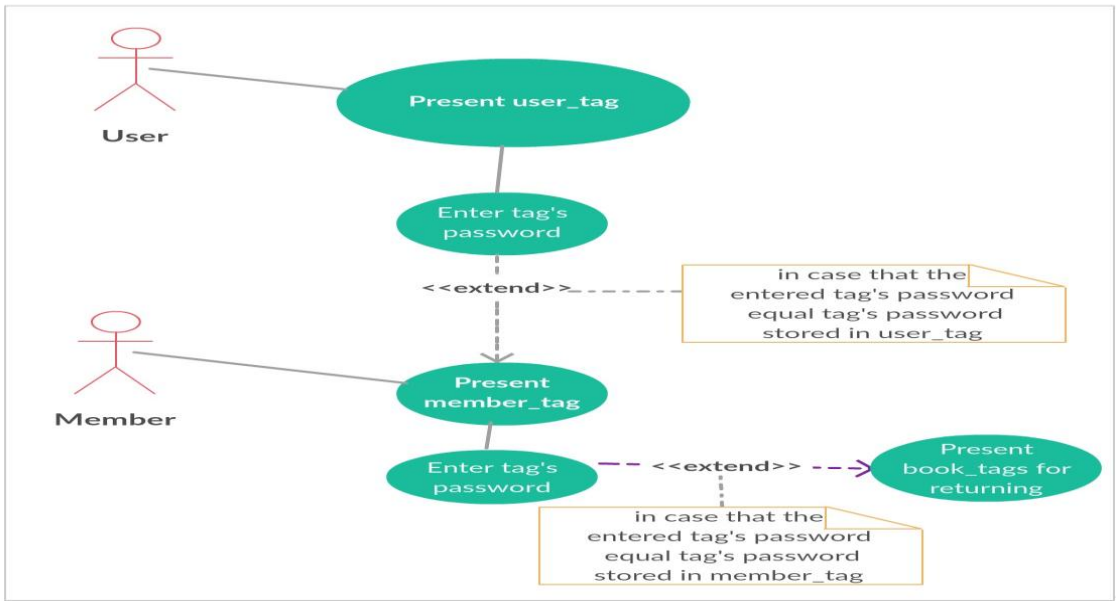

Figure 17 Use Case Diagram for Books Returning Module (Interaction with User and Member).

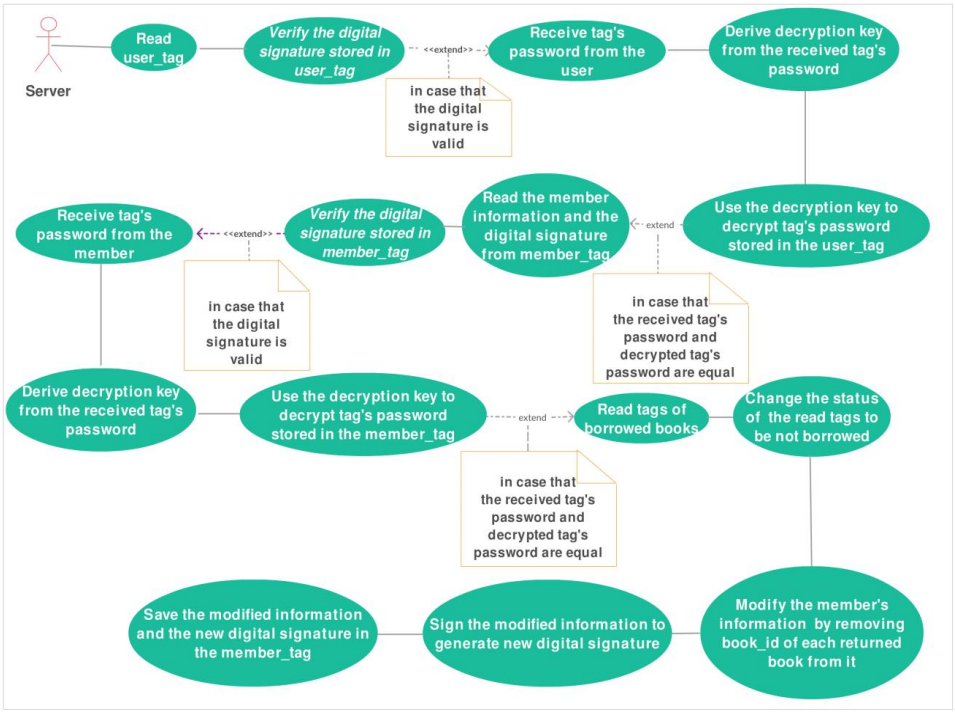

Figure 18 Use Case Diagram for Books Returning Module (Interaction with Server).

4.6. Books Monitoring Module

The books monitoring module is used to track the books at the exit door of the library. Here, the module continuously reads the book-tags to checks the digital signatures and the masking bits of the books. If any masking bit is active (true) or the digital signature is invalid, then the module starts the alarming system. The alarming is continuing until a system's user removes the alarming state by issuing ignore command to the book monitoring module.

5. Conclusion

The Internet has changed drastically the way of living, moving interactions between people at a virtual level in several contexts spanning from the professional life to social relationships. The IoT has the potential to add a new dimension to this process by enabling communications with and among the things around us by using smart devices such as Radio-Frequency Identification (RFID) tags, sensors, mobile phones, etc., thus leading to the vision of ‘‘anytime, anywhere, anything” communications. The RFID technology stands at the forefront of the technologies driving the IoE/IoT vision. However, using RFID technology has bleeding edges in adopting it for sensitive applications because RFID still has security issues; namely: privacy protection, impersonation, and data integrity. Security is an integral part of any sensitive application, as a result, addressing the security issues is the first step in developing such application. This paper proposed an improvement to a three pass authentication protocol to address the security issues of passive RFID. The improved protocol uses the digital signature and password based encryption schemes to solve the security issues. The improved protocol is adopted to design a secure E-library management system. As a part of our future work, we will give a concrete implementation of the SELMS at the University of Baghdad Libraries.

References

1. Muhic, I., and Hodzic, M. (2014). Internet of Things: Current Technological Review and New Low Power Wireless Sensor Network Protocol Proposal. Southeast Europe Journal of Soft Computing, 3(2), pp. 46–57.
2. Lee, D. (2016). Study on Actual Cases & Meanings for Internet of Things. International Journal of Software Engineering and Its Applications, 10(1), pp. 287–294.
3. Amendola, S., Lodato, R., Manzari, S., Occhiuzzi, C., and Marrocco, G. (2014). RFID Technology for IoT-Based Personal Healthcare in Smart Spaces. IEEE Internet of Things Journal, 1(2), pp. 144–152.

4. Aydin, K. and Yildirim, S. (2012). A Case Study about RFID Technology Usage in Library Services. JGSM, 2(6), pp. 113–113.
5. M, D. and Mamatha, U. (2009). RFID Based Library Management System. Proceedings of ASCNT, pp. 227-234.
6. Younis, M. I. (2012). SLMS: A Smart Library Management System based on an RFID Technology. International Journal of Reasoning-based Intelligent Systems, 4(4), pp. 186–191.
7. Bansode, S. and Desale, S. (2009). Implementation of RFID Technology in University Of Pune Library. Program: Electronic Library and Information Systems, 43(2), pp. 202–214.
8. Yu, D. (2011). Implementation of RFID Technology in Library Systems Case Study: Turku City Library. Lahti University of Applied Sciences.
9. Yang, D., Liu, F. and Liang, Y. (2010). A Survey of the Internet of Things. Proceedings of the 2010 International Conference on E-Business Intelligence.
10. Peris-Lopez, P., Hernandez-Castro, J., Estevez-Tapiador, J. and Ribagorda, A. (2006). LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID Tags. Proc. Second Workshop RFID Security.
11. Peris-Lopez, P., Hernandez-Castro, J., Estevez-Tapiador, J. and Ribagorda, A. (2006). M2AP: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags. Ubiquitous Intelligence and Computing, pp. 912–923.
12. Chien, H. (2007). SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. IEEE Transactions on Dependable and Secure Computing, 4(4), pp. 337–340.
13. Peris-Lopez, P., Hernandez-Castro, J., Tapiador, J. and Ribagorda, A. (n.d.). Advances in Ultralightweight Cryptography for Low-Cost RFID Tags: Gossamer Protocol. Information Security Applications, pp. 56–68.
14. Srivastava, K., Awasthi, A., Kaul, S., and Mittal, R. (2014). A Hash Based Mutual RFID Tag Authentication Protocol in Telecare Medicine Information System. J Med Syst, 39(1).
15. Zhou, J. (2015). A Quadratic Residue-Based Lightweight RFID Mutual Authentication Protocol with Constant-Time Identification. Journal of Communications, 10(2), pp. 117–123.
16. Sun, H. and Ting, W. (2009). A Gen2-Based RFID Authentication Protocol for Security and Privacy. IEEE Transactions on Mobile Computing, 8(8), pp. 1052–1062.
17. Ha, J., Moon, S., Nieto, J. and Boyd, C. (n.d.). Low-Cost and Strong-Security RFID Authentication Protocol. Emerging Directions in Embedded and Ubiquitous Computing, pp. 795–807.
18. Barasz, M., Boros, B., Ligeti, P., Loja, K. and A. Nagy, D. (2007). Breaking LMAP. Proc. of RFIDSec 2007, pp. 11–16.
19. Li, T., Wang, G. and Deng, R. (2008). Security Analysis on a Family of Ultra-lightweight RFID Authentication Protocols. JSW, 3(3), pp. 1–10.

20. D'Arco, P. and De Santis, A. (2008). From Weaknesses to Secret Disclosure in a Recent Ultra-Lightweight RFID Authentication Protocol. IACR Cryptology ePrint Archive 2008, 5023, pp. 27–39.
21. Bilal, Z., Masood, A. and Kausar, F. (2009). Security Analysis of Ultra-lightweight Cryptographic Protocol for Low-cost RFID Tags: Gossamer Protocol. 2009 International Conference on Network-Based Information Systems, pp.260–267.
22. Ozcanhan, M. (2015). Analysis of a Recent Hash Based RFID Authentication Protocol Intended for Telecare Medicine. IRJET, 2(4), pp. 1520–1524.
23. Ozcanhan, M. (2015). Analysis of a Recent Quadratic Residue Based Authentication Protocol for Low-Cost RFID Tags. International Journal of Novel Research in Engineering and Science, 2(1), pp. 7–13.
24. Vahedi, E., Ward, R. and Blake, I. (2011). Security Analysis and Complexity Comparison of Some Recent Lightweight RFID Protocols. Computational Intelligence in Security for Information Systems, pp. 92–99.
25. van Deursen, T. and Radomirović, S. (2009). Security of RFID Protocols – A Case Study. Electronic Notes in Theoretical Computer Science, 244, pp. 41–52.
26. Semiconductors, N. X. P. (2007). Mifare Standard 4KByte Card IC Functional Specification.
27. Gans, G. (2008). Analysis of the Mifare Classic Used in the OV-Chipkaart Project. Radboud University Nijmegen.
28. de Koning Gans, G., Hoepman, J. and Garcia, F. (2008). A Practical Attack on the Mifare Classic. Smart Card Research and Advanced Applications, pp.267–282.
29. Liao, H. and Shen, Y. (2006). On the Elliptic Curve Digital Signature Algorithm. Tunghai Science, 8, pp. 109–126.
30. Khalique, A., Singh, K. and Sood, S. (2010). Implementation of Elliptic Curve Digital Signature Algorithm. International Journal of Computer Applications, 2(2), pp. 21–27.
31. Barker, E., and Roginsky, A. (2015). Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths. NIST Special Publication 800-131A.
32. Abdalla, M., Fouque, P. A., and Pointcheval, D. (2006). Password-based Authenticated Key Exchange in the Three-Party Setting. IEE Information Security, 153(1), pp. 27–39.
33. Atreya, M. (n.d.). Password Based Encryption. [Online]. Available at: https://web.cs.ship.edu/~cdgira/courses/CSC434/Fall2004/docs/course_docs/Article3-PBE.pdf [Accessed 5 Mar. 2016].

تصميم وتطبيق نظام ادارة مكتبة الكترونية آمن

أ.م.د. محمد عصام يونس* **مصطفى هاشم عبدالكريم***

المستخلص

لقد غير الانترنت الطريقة التي نعيشها بشكل كبير ، ناقلاً التفاعلات بين الناس على المستوى الافتراضي سياقات متعددة متوسعة من الحياة المهنية الى العلاقات الاجتماعية. انترنت الاشياء لديه القدرة على اضافة بعد جديد لهذه العملية من خلال تمكين الاتصالات مع وبين الاشياء من حولنا باستخدام الاجهزة الذكية مثل اجهزة التعريف باستخدام الموجات الراديوية، اجهزة الاستشعار، الهواتف المحمولة، الخ مما يؤدي الى رؤية الاتصالات "في أي وقت، في أي مكان، أي شيء". تقنية التعريف باستخدام الموجات الراديوية تقف في طليعة التقنيات التي تقود تلك الرؤية، ومع ذلك فان استخدام هذه التقنية في التطبيقات الحساسة لايزال يعاني من مشاكل الامن والخصوصية. هذا البحث يتناول مشاكل الامن والخصوصية ويقترح نظام ادارة مكتبة الكترونية آمن بالاعتماد على التعريف باستخدام الموجات الراديوية وباستخدام التوقيع الرقمي وخدمات التشفير الاخرى لجعل اعتماد هذه التطبيقات الحساسة عملياً أكثر.

*جامعة بغداد