Mutual Chain Authentication Protocol for SPAN Transactions in Saudi Arabian Banking

S. Nashwan and B. Alshammari

***Abstract*—Numerous examinations of the weaknesses with current two-factor-authentication (2FA) protocol of Automated Teller Machines (ATMs) systems have been presented by various researchers. It is plausible to suggest that the majority of the proposed solutions of authentication protocols in the reported investigative works are formulated based on Biometrics protocol as access control mechanism. Those aim to protect and validate the privacy of information of users or ATM cards. Most of the financial institutions in Saudi Arabia are still hesitate to use any of these proposed protocols. This is due to the user's mentality to use new technology and the complexity of these systems. This paper proposes a new Mutual Chain Authentication Protocol (MCAP) for the Saudi Payments Network (SPAN) transactions in the Saudi Arabian banking. MCAP is resistant against the well-known communication attacks of the current authentication protocols and it does not contradict with the mentality of users and at the same time preserves the current ATMs system entities.**

***Index Terms*—ATM systems, SPAN, authentication, key agreement protocol (AKA).**

I. Introduction

The Saudi payments network (SPAN) is the National ATM and Points of Sale (POS) network connecting all Saudi banks and providing a common service point to the Kingdom [1]. The SPAN is operated by Saudi Arabian Monetary Agency (SAMA). It processes all POS transactions in Saudi Arabia and also all cross-bank ATM transactions.

The ATM service was introduced in 1990 with the POS service being added in 1993 [2]. By the end of 2010, the Saudi Arabian commercial banks had issued more than 12 million eligible and active cards which can function as both ATM and POS cards [2]. SPAN had processed ATM transactions to the value of SAR 468 billion in 2010 (about 40% of all ATM transactions – the remainder being in-house transactions at the issuing banks' own ATMs).It had also processed POS transactions to the value of SAR 72 billion (all POS transactions are processed through the central switch) with an average SAR 475.32 per transaction [2]. There are almost 10,900 ATM terminals and more than 80,000 POS terminals in Saudi Arabia. Furthermore, there are 16 direct participants in SPAN which operates around the clock [2].

Therefore, there is a growing need in Saudi Arabia to implement a secure authentication protocol for ATMs system. This aims to ensure that financial transactions or exchanging of sensitive financial data are executed in a secure manner. Although there is a huge demand in Saudi Arabia to use ATM card users and ATM services compared to the neighboring countries in the region, it is worth mentioning that most of the users in Saudi Arabia are convenient with the traditional ATM authentication protocol. Moreover, a significant number of users are not aware about ATM frauds despite of the increasing number of incidents of ATM frauds which were occurred in the Saudi Arabia [3].

Since many of the existing ATM machines are secured with the two-factor authentication protocol, several works have been done to overcome its weaknesses [4]–[7]. These weaknesses can be divided into two main categories; one is related to the access method which concentrates on securing the data between the user and the machine. The other weakness is related to insecure communication during the exchange of the authentication messages between authentication entities which can lead to the traffic analysis attacks. Most of the research in this area concentrates on modifying the authentication protocol by changing the kernel function to be based on Biometrics protocol to be against card and currency fraud attacks such as ATM card skimming attack and card trapping/fishing attack [8]–[14]. Most of the financial institutions in Saudi Arabia are still doubtful to use any of these proposed protocols instead of the current authentication protocol. This is due to a number of reasons including: users' hesitance to use new technology; cost of adding new hardware, and complexity of new software.

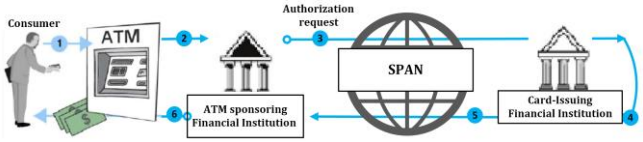

Fig. 1. Authentication entities of ATM systems.

Fig. 1 shows the authentication entities of an ATM system in Saudi Arabia. The authentication protocol is managed by the SPAN entity. In the first step, the users insert their cards into the ATM terminal, thereby allowing ATM terminal to obtain the card specifications. Step 2, the ATM terminal forwards information read from the ATM card along with the user's request message to the sponsoring bank of the ATM terminal. In step 3, the sponsoring bank forwards this information to SPAN, which routes the request message to the card issuing of financial institute according to the card information. However, this step is only executed when the ATM card doesn't belong to the ATM sponsoring financial institution. Step 4, the card-issuing financial institute verifies the identity of the ATM terminal and card specifications from its database. It then processes the transaction of the cardholder. Step 5, the card-issuing financial institute entity

Manuscript received February 9, 2014; revised April 25, 2014.

The authors are with the Computer Information System Department at Al jouf University (e-mail: shadi_nashwan@ju.edu.sa, bmshammeri@ju.edu.sa).

sends an authorization response message to the SPAN entity, which routes the response message to the ATM sponsoring bank entity. Finally, in step 6 the ATM terminal dispenses the request service to the user after receiving the authorization response message from the sponsoring bank entity.

A major threat in such ATM systems is that communication between authentication entities might be exposed to an attack. An unauthorized party might be able to access the authentication messages that have been sent between communication entities (ATM machine, sponsoring bank, SPAN and card-issuing financial institute). An attacker can passively capture the authentication messages without trying to analyze the content, at a later time the same authentication request message is used in the same sequence to impersonate an event and gain unauthorized access to the user account. Furthermore, an unauthorized party can also delete all contents of the authentication message and then replace it by counterfeited messages.

Therefore, this paper proposes a new authentication protocol for ATM systems called Mutual Chain Authentication Protocol (MCAP). It aims to be highly resistant against communication attacks such as the replay attack, the personalization attack, the guessing attack, and the man-in-the-middle attack. It also has to meet the ATM Security Specifications described in [15]–[17]. The MCAP is developed based on Authentication and Key Agreement protocol (AKA) concepts [18], [19].

In MCAP, the system authentication entities are prevented from sending any authentication parameters as clear text. Instead, the kernel functions generate Message Authentication Code (MAC) value to guarantee the freshness and legality of the authentication messages and to achieve the mutual authentication between all authentication entities.

The remainder of this paper is organized as follows. Section II provides a summary of existing research which discusses mutual authentication protocols in the literature. Section III introduces the core functions and the main authentication parameters of the MCAP. The detail of the authentication processes in each authentication entities (the ATM terminal, the sponsoring bank of the ATM terminal (SBAT), SPAN, and card-issuing financial institute (CIFI)) are discussed in Section IV. In Section V, the security analysis of the proposed protocol is discussed. Finally, Section VI summarizes the salient results of the proposed protocol.

II. Related Work

Cryptography provides the necessary tools for accomplishing secure and authenticated transactions. It doesn't only protect the data from theft or alteration, but can also be used for user authentication. The majority of the proposed solutions of authentication protocols which focus on protecting and validating the privacy of user's information or ATM cards in ATM systems are formulated on biometrics access methods.

The main focus of the work of Suneel *et al.*'s [20] is to make the ATM machine more secure by providing dual security (i.e., fingerprint recognition and entering password). So, to overcome the above problems they have designed a system with a finger print reader and keypad which is useful for entering a password without using ATM cards. Once the finger details are given, a window is displayed on the controller that contains keypad and using that keypad a user can enter the password after being enrolled. Person can enter the amount to withdraw and receive notes from note dispenser (stepper motor) interfaced with microcontroller.

In the work of Mohammed's [21], he provided an overview of the possible fraudulent activities that may be perpetrated against ATMs and recommended approaches to prevent these types of frauds. A prototype model for the utilization of biometrics equipped in an ATM is developed to provide security solution against the well-known breaches. Han's et al had studied the smartcard based on fingerprint encryption/authentication scheme for ATM banking systems [22]. In this scheme, a system authenticates users by both their possession (smartcard) and biometrics (fingerprint). A smartcard is used for the first layer of authentication. Based on the successful pass of the first layer authentication, a subsequent process of the biometric fingerprint authentication is preceded.

The work of Oko and Oruh [23] aims to improve the security of ATM systems by integrating the fingerprint of a user into the bank's database in order to authenticate it. This was achieved by modeling and building an ATM simulator that is mimicked a typical ATM system. The main objective result of this work is to increase customers' confidence in the banking sector. Ndife *et al.* have developed an Automated Fingerprint Identification Machine (AFIM) to enhance the performance and security of bank customers [24]. This work had adopted the software development lifecycle (SDLC) as well as secured hashing algorithm (SHA) to determine the interface between the scanner and the proposed system, and the threshold of the scan fingerprint image. However, the model implementation of this research showed robustness in security and service delivery performance.

From the above literature review, it can be seen that biometric systems can offer convenient and secure mode to achieve authentication just between the ATM card and ATM terminal in a one way manner. However, this approach lacks of providing a secure integration view to the rest of the authentication entities in an ATM system during the SPAN transactions. Therefore, this paper proposes a new authentication protocol based on the AKA concepts without taking into account the biometric methods to achieve the mutual authentication. The proposed protocol can also strengthen security against the well-known communication attacks between all authentication entities.

III. MCAP Functions and Authentication Parameters

The authentication protocol is one of the most important services in any ATM system as all other services are based on it. Since no higher level services can be used without an authentication between the communication entities, the MCAP is fulfilled with a set of symmetric cryptography functions and parameters. One of these is $f0$ which represents a random challenge-generating function and it should be a (pseudo) random number-generating function. The output of

this function is a challenge value RAND that is executed in the ATM terminal to initiate the authentication session.

TABLE I: AUTHENTICATION FUNCTIONS AND THEIR OUTPUTS

Function	Description	Output
*f*0	The random challenge generating function	RAND
*f*2,*f*1,*f*10, *f*3*,*f*11*	ATM terminal functions	XRES1/XACI/XRES2 / RAND+1/AMID
*f*10*, *f*11, *f*6*,*f*4	SBAT functions	SQNATMS/RES2/ AMID/XRES4/
*f*5*,*f*4*, *f*6,*f*5	SPAN functions	SQNCS, SQNSS, RES3,XRES4
*f*1*,*f*2*,*f*12, *f*12*,*f*3	CIFI functions.	ACI/RAND/RES4/ AMID/RES1
*f*7.	Temporary ACI function	TACI
*f*8, *f*9.	The cipher and integrity keys functions in ATM terminal and SBAT	CK,IK

TABLE II: INPUT AND OUTPUT AUTHENTICATION PARAMETERS

Authentication Parameters	Definition
K1.	Pre-shared Secret Key (ATM card , CIFI)
K2.	Pre-shared Secret Key (ATM card , SBAT)
K3.	Pre-shared Secret Key (SPAN , CIFI)
K4.	Pre-shared Secret Key (SBAT , SPAN)
ACI.	ATM Card Identity
RAND.	Random Challenge
AMID.	ATM Terminal Identification
XACI.	Expected ACI
TACI.	Temporary ACI
RES1, RES2, RES3, RES4	Expected Response
XRES1, XRES2, XRES3, XRES4.	Expected Challenge
CK, IK.	Cipher and Integrity Keys
SQNATM, SQNSS, SQNCS.	Sequence Number of Transaction of /ATM Terminal/SBAT/CIFI

Functions *f* 1, *f* 1*, *f* 2, *f* 2*, *f* 3, *f* 3*, *f* 5, *f* 5*, *f* 6, *f* 6*, *f* 10, *f* 10*, *f* 11, *f* 11*, *f* 12 and *f* 12* are challenge-response functions that are executed in authentication entities to achieve a mutual authentication between these entities. Function *f* 7 is executed to generate a temporary identification value for the ATM card. Both of functions *f* 8 and *f* 9 are executed to generate cipher and integrity keys. A detailed description of these functions and their output are shown in more detail in Table I. Table II shows the MCAP parameters and their definitions.

The structure of the MCAP is based on the concepts of AKA [18] which include mutual authentication and key agreement. The mutual authentication means that users identify and prove themselves to the system and the same thing for the opposite direction in which the system identifies and proves itself to the user [19]. The key agreement means that communication entitles agree on the keys that are related to the ciphering and integrity services [19]. Therefore, when the MCAP processes are completed, this leads to achieve integrity protection of messages service, confidentiality protection for both of signaling data and user data services, and, hence, mutual authentication is reached between all communication entities.

IV. MCAP FUNCTIONS IMPLEMENTATION

This section illustrates the authentication processes in the ATM terminal, the sponsoring bank of the ATM terminal (SBAT), SPAN, and card-issuing financial institute (CIFI) in more detail.

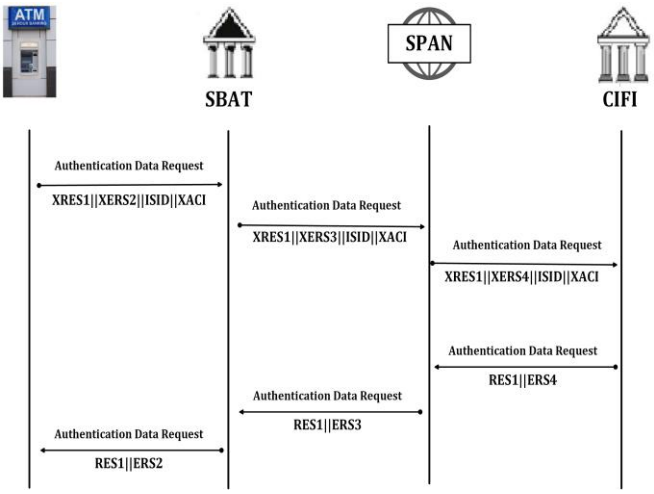

Fig. 2. Authentication protocol sequence diagram.

Fig. 2 shows the sequence diagram of MCAP in all authentication entities. The authentication data request message that is sent from the ATM terminal through SBAT, includes (XACI), (XRES1), (XRES4), (AMID) and the Initial Session identification (ISID), is sent by SPAN to ICFI. ICFI retrieves necessary data using the (ISID) to generate the RES1and RES4 values. It then responds to SPAN by sending an authentication data response message which includes RES1 and RES4. SPAN sends a user authentication response message to SBAT which SBAT passes to the ATM terminal. Specifically, SPAN sends RES1 value through SBAT to the ATM terminal. The latter verifies the value of (RES1) by comparing it with (XRES1).

A. ATM Terminal

Card holders insert their cards into the ATM terminal, thereby allowing ATM terminal to obtain the card specifications. The ATM terminal starts the authentication processes by sending an authentication data request message that includes the (ISID) of the ATM card, (XACI), (XRES1), and (XRES2) to SBAT.

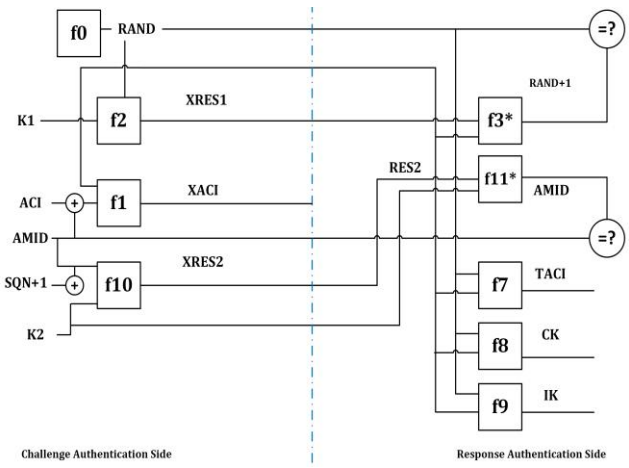

Fig. 3. Challenge and response authentication function in ATM terminal.

This message is considered a declaration message to request service permission from the CIFI. This message helps the card holder and the ATM terminal to prove their identity to the system. At the same time, the system ensures that the message is not altered during the transmission based on the AMID and ACI values which are encrypted in the message with the output of $f1$, $f2$, and $f10$ functions. These processes are executed in series of steps as shown in the challenge authentication side in Fig. 3.

1) The first component in an authentication request message is the (ISID) which represents the (ID) of the ATM card that is used the first time the ATM card requested the authentication services.
2) The second component of the authentication request message is the (XACI) which represents the output of function $f1$. The $f1$ function consists of the following input parameters; AMID (ATM terminal Identification) and (ACI) of the ATM card. It can be represented using the following formula.

$$(f1 = EK1(AMID \oplus ACI) = XACI)$$

3) The third component of the authentication request message is the (XRES1) which represents the output of function $f2$. The $f2$ function takes a single input (RAND) that is generated by the ATM terminal using $f0$ function. It can be represented using the following formula.

$$(f2 = EK1(RAND) = XRES1)$$

4) The the fourth component is the (XRES2) which represents the output of function $f10$. Function $f10$ consists of the following input parameters (SQNATMS + 1: next Sequence transaction number between ATM terminal and SBAT) and (AMID). It can be represented using the following formula.

$$(f10 = EK2((SQNATMS + 1) \oplus AMID) = XRES2)$$

After the ATM terminal receives the authentication response message from SBAT which includes (RES1) and (RES2), ATM terminal checks the validity and authenticity of the message. It uses $f11^*$ and $f3^*$ decryption functions and executes the following steps as shown in the response side in Fig. 3.

1) ATM terminal verifies the value of (RES2) which is used to authenticate the legality of SBAT using the following formula.

$$(f11^* = DK2(RES2) = AMID))$$

2) ATM terminal verifies the (RES1) value which is used to authenticate the legality of CIFI using the following formula.

$$(f3^* = DK1(RES1) = (RAND + 1))$$

By comparing the decrypted values of (RES1) and (RES2) that are delivered from the SBAT and CIFI with the encrypted values of (XRES1) and (XRES2), the system decides to proceed with the service or decline it. In case the system authentication fails, then this means that the challenge is received from an illegal party (CIFI, SAPN and SBAT) or it may be that the message is altered during transmission. Therefore, the ATM terminal will reject it and send authentication failure report to the CIFI through the SBAT and SPAN.

3) ATM terminal encrypts the value of (RAND) that is XORed with (ACI) to generate the (TACI) (i.e., function $f7$). This will be stored in the ATM card and (TACI) is used in next authentication session using the following formula.

$$(f7 = EK1(RAND \oplus ACI)$$

4) ATM terminal encrypts the value of (RAND) to generate the cipher key using derivation function ($f8$). Function $f8$ takes the subscriber key (K1) and the random challenge (RAND) as inputs and produces the (CK) as output using the following formula.

$$(f8 = EK1(RAND = CK)$$

5) ATM terminal encrypts the value of (RAND) to generate the integrity key using derivation function ($f9$). Function $f9$ takes the subscriber key (K1) and the random challenge (RAND) as inputs and produces (IK) as output using the following formula.

$$(f9 = EK1(RAND = IK)$$

B. The Sponsoring Bank of the ATM Terminal (SBAT)

After the ATM terminal forwards the authentication request message to the sponsoring bank of the ATM terminal SBAT, SBAT checks the authenticity of the message. It then directly checks the (SQNATMS) of the ATM terminal whether out of range or not by executing function $f10^*$ which is represented by the following formula.

$$(f10^* = DK2(XRES2) = ((SQNATMS + 1) \oplus AMID))$$

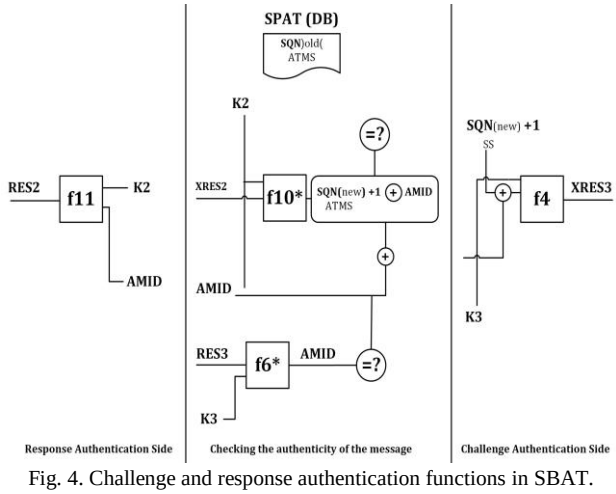

Fig. 4. Challenge and response authentication functions in SBAT.

Function f 10* aims to compute the value of SQNATMS, then adds the value of AMID which is computed using (((SQNATMS +1) $\oplus$ AMID $\oplus$ AMID), = SQNATMS +1), then compares it with the old value of SQNATMS that has stored in the database. If they are not equal then a failure message is sent back to the ATM terminal, see checking the authenticity of the message side in Fig. 4. The SBAT verifies that the ISID of ATM card to decide if the transaction will be executed locally or through the SPAN. If the ATM terminal follows another financial institute entity, SBAT executes function f 4 which can be represented by the below formula.

$$f4 = EK3((SQNSS + 1) \oplus AMID)$$

It adds both of XRES3 and AMID values to the authentication request message and passes the message to SPAN, see challenge authentication side in Fig. 4. When SBAT receives the authentication response message which includes the (RES1) and (RES3) from SPAN, the SBAT checks the validity and authenticity of the authentication parameter (RES3) that have been received from SPAN by decrypting (RES3) value using function f 6. Function f 6 can be represented by the following formula.

$$(f6^{*} = DK3(RES3) = (AMID))$$

The validity of the RES3 is checked by comparing both values (AMID) and (the output f 6* AMID that is encrypted by SPAN using f 6) as shown in the response authentication side in Fig. 4. The SBAT adds the value of RES2 using (f 11 = EK2 (AMID) = RES2). It then sends back the authentication response message to the SBAT which includes (RES1) and (RES2) as shown in the response authentication side in Fig. 4.

C. SPAN

After SPAN receives the authentication request message from the sponsoring bank of the ATM terminal (SBAT), it asks the authentication server to determine both of SBAT and ICIFI using the values of (ISID) and (AMID). The authentication server retrieves the entire authentication data which consists of old SQN of SBAT, shared key (K3), and shared key (K4).

SPAN checks the authenticity of the message and checks the (SQNSS) of the SBAT whether out of range or not. Thereafter, SPAN executes function f 4* to compute the value of SQNSS. Function f 4* can be represented by the following formula.

$$(f4^{*} = DK3(XRES3) = ((SQNSS + 1) \oplus AMID)))$$

SPAN then adds the value of AMID that is included in the authentication request message by SBAT using (((SQNSS +1) $\oplus$ AMID $\oplus$ AMID), = SQNSS +1). It then compares it with the old value of SQNSS that has been stored in the database. If these two values are not equal, then a failure message is sent back to the SBAT. This is shown in the authenticity checking of the message side in Fig. 5.

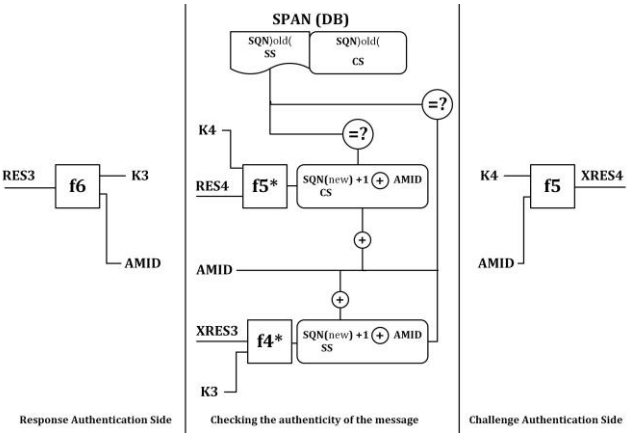

Fig. 5. Challenge and response authentication functions in SPAN.

Furthermore, the SPAN adds the value of XAMID using function f 5, which is shown below.

$$(f5^{*} = EK4(AMID) = XRES4)$$

SPAN then routes the authentication request message to the desired ICFI of the ATM card according to the value of first four digits.

When SPAN receives the authentication response message that includes (RES1) and (RES4) from CIFI, it requests the authentication server to retrieve the old SQN of CIFI value. It then checks the validity and authenticity of the authentication parameters that have been received from CIFI by decrypts (RES4) value using function f 5*.

$$(f5^{*} = DK4(RES4) = (AMID \oplus SQNCS + 1))$$

Function f 5* computes the value of SQNCS, it then adds the value of AMID using (((SQNCS +1) $\oplus$ AMID $\oplus$ AMID), = SQNCS +1). Subsequently, it compares this value with the old value of SQNCS that has been stored in the database. If these two values are not equal then a failure message is sent back to the CIFI. The SPAN adds the value of RES3 according using function f 6, which is represented by the following formula.

$$(f6 = EK3(AMID) = RES3)$$

It then sends back the authentication response message to the SBAT that includes (RES1) and (RES3).

D. Card-Issuing Financial Institute (CIFI)

When CIFI receives the authentication request message from SPAN, it requests the authentication server, which has stored the authentication data of the ATM card, to generate RES1. The authentication server uses (ISID) to retrieve the whole authentication data which includes ACI and shared key (K1) of the ATM card. The authentication request message from SPAN includes the following parameters. One is the XRES4 value which is added by the SPAN to prove itself to CIFI using the spatial shared key between K4. The other parameters include (ISID), (XACI), (AMID) and (XRES1). All of these parameters are used to achieve the mutual authentication between the ATM terminal-CIFI, SBAT-CIFI,

and SPAN-CIFI. Therefore, the first step of the authentication processes in the CIFI is to check the validity and authenticity of the authentication parameters that have been received from SPAN (see Fig. 6).

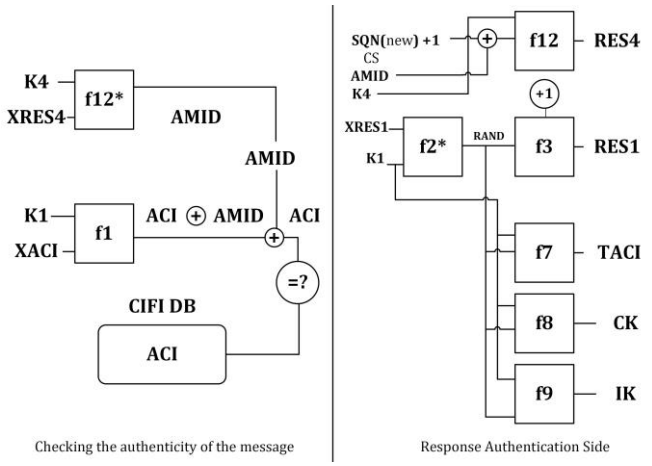

Fig. 6. Challenge and response authentication functions in CIFI.

The authentication functions which are used in the CIFI are executed in the following two steps:

1) CIFI decrypts the value of (XRES4) using function f12* to retrieve the value of (AMID) of the ATM terminal. Function f12* is represented by the following formula.

$$(f12^{*} = DK4(XRES4) = (AMID))$$

2) Then CIFI decrypts the value of (XACI) using function f 1* to retrieve both (ACI) of the ATM card and the value of the (AMID) using the following formulas.

$$(f1^{*} = DK1(XACI) = AMID \oplus ACI)$$

It then (AMID⊕ AMID⊕ ACI) = ACI, then compares both of (ACI == ACI) and (AMID = = AMID). Through step 1 and step 2, CIFI checks the validity of the XACI) and (XRES4). CIFI compares the values of (ACI) and (AMID) that were received from SBAT with those added from SBAT. Therefore, ATM terminal, SBAT and SPAN identify themselves to CIFI.

3) CIFI uses function f 2* to decrypt the value of (XRES1) to retrieve the value of (RAND) using function f 2* as shown in the following formula.

$$(f2^{*} = DK1(XRES1) = RAND)$$

It then encrypts the value equal to (RAND +1), then executes function f 3 which is represented by the below formula.

$$(f3 = EK1(RAND + 1) = RES1)$$

This function aims to generate and send the (RES1) parameter back to the ATM terminal. CIFI by the (RES1) value proves itself to the ATM terminal.

4) CIFI executes function f12 to generate (RES4) and sends it back to SPAN. By doing so, CIFI proves itself to SPAN. Function f12 can be represented by the following formula.

$$(f12 = EK4(AMID \oplus SQNCS + 1) = (RES4))$$

5) CIFI Generates the value of temporary identification (TACI) using function f7 according to the below formula.

$$(f7 = EK1(RAND \oplus IACI) = TACI)$$

The ATM card by (TACI) during the next authentication session will identify itself to the system without using ISID.

6) CIFI Encrypts the value of (RAND) to generate the cipher key using derivation function f8 as shown in the below formula.

$$(f8 = EK1(RAND) = CK)$$

This function takes the subscriber key (K1) and the random challenge (RAND) as inputs and produces the (CK) as output.

7) CIFI Encrypts the value of (RAND) to generate the integrity key using derivation function f9 as shown in the following formula.

$$(f9 = EK1(RAND) = IK)$$

This function takes the subscriber key (K1) and the random challenge (RAND) as inputs and produces the (IK) as output.

8) The CIFI sends back the authentication response message which includes (RES1) and (RES4) to SPAN.

V. Security Analysis of the MCAP Protocol

This section aim to prove that MCAP authentication protocol has achieved the security requirements of ATM systems by adding a set of security features to the current authentication protocol. In MCAP, the security level of all services in the ATM systems (the mutual authentication, the key agreement, the key confirmation, the anonymity, the confidentiality, and the non-repudiation) are achieved in such a way much more than the security level of the current authentication protocol.

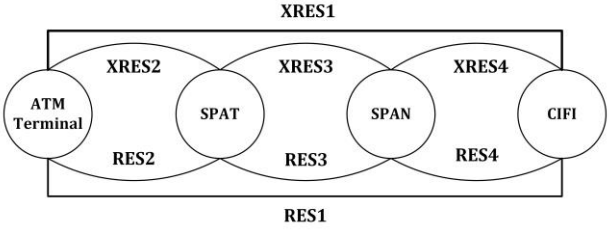

Fig. 7. Challenge/response authentication messages sequence diagram.

Mutual authentication between all communicating parties has been achieved by executing a set of challenge/response messages. Fig. 7 shows the Sequence diagram of the Challenge/Response Authentication messages.

The mutual authentication between ATM terminal and

CIFI depends on the values of XRES, XACI and RES1. ATM terminal executes f 1 and f 2 to compute XRES1 and ACI based on the pre-loaded shred key K1 to identify itself to the CIFI. In the opposite direction, CIFI executes f 3 to compute RES1 based on the same encryption key K1 to identify itself to ATM terminal.

The mutual authentication between all authentication entities is represented by chain of Challenge and Response messages [(XRES2/RES2), (XRES3/RE3) and (XRES4/RES4)]. This chain depends on the values of SQN parameters that are stored in ATM terminal. SBAT and CIFI databases also depend on the AMID parameter that is added to the authentication request message by SBAT entity.

In each time the challenge message is forwarded to the next entity, the authentication entity checks the freshness of SQN parameter. It does this by comparing the SQNnew extracted from the decryption value of XRES with the value of SQNold that is stored in the DB of the authentication entity. If the SQNnew is in range then passes the authentication request to the next authentication entity. Otherwise, a failure authentication message is sent back. In the opposite direction, the authentication entity checks the AMID value by comparing the AMID that is extracted from the decryption value of RES with the value attached to the authentication request message. If these are not identical, then a failure authentication message is sent back.

The outputs of the authentication functions between all authentication entities are completely encrypted by EK1, EK2, EK3 and EK4 for all authentication events. The Confidentiality is achieved in the MCAP through protecting all messages that have been transmitted from eavesdropping; all authentication messages have contained the encrypted parameters; which are encrypted by the kernel functions using the pre-loaded shared keys without exchange the value of the keys between the authentication entities. The Cipher key (CK) and the integrity key (IK) have never been exchanged between the communication entities. Furthermore, the proposed protocol is unlike existing authentication protocols as it doesn't allow sending pairs of plaintext-ciphertext. This prevents attackers from threatening the security level and lower bound complexity of the cryptography algorithm that is used.

Anonymity service in communication ensures that no one else other than the intended communication parties is able to figure out who is communicating with whom [25]. In each time the MCAP is executed, the encrypted value of (ACI) in authentication request messages will change in the first authentication session. One of the goals of using (AMID) as an input value to function f 1 in ATM terminal side is to change the encrypted value of the (ACI) according to the value of AMID. This is considered as the perfect solution to concealment (ACI); where (AMID) is changed in each time the card holder moves from an ATM terminal to another.

The MCAP is resistant against the personalization attack after the authentication session is executed. Both of ATM terminal and CIFI will use the value of (TACI). Therefore, the true identity of the ATM card in the proposed protocol cannot be discovered by an attacker eavesdropping over the radio access link interface.

The MCAP also guarantees to achieve the non-repudiation security property by ensuring that no party can deny their actions after the completion of their communication [25]. The ATM card contains unique identifiers (ACI) and secret key. Therefore, both unique values together are considered as evidence that no one can deny their actions.

The proposed protocol is resistant against the Man-in-the-middle attack. The man-in-the-middle is a form of active attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association. The cryptography algorithm as kernel functions protect the authentication messages against any data-modifying because the correct secret keys are only known by the authentication entities.

The proposed protocol is resisted against the replay attack [25]. The replay attack is that valid data transmission is maliciously or fraudulently repeated. This can be done by either the originator or an adversary who intercepts the data and retransmits it. One of the main input parameters in all authentication entities kernel function is the SQN values. These values are change in a sequence manner for each authentication transaction. If the attacker intercepts the authentication request message and retransmits it at a later time to the authentication entities without modifying its content, a rejection authentication message is sent back. This is when the value of SQN is considered expired.

VI. Conclusion

This paper proposes a new Mutual Chain Authentication Protocol MCAP for the SPAN transactions in Saudi Arabia banking. It aims to overcome existing weaknesses in the current authentication protocol and to meet the ATM system security specifications.

In MCAP, no authentication parameters are transmitted as a plaintext through the authentication messages between the authentication entities. Therefore, it enhances the security level of the confidentiality service in a way that is comparatively better than other similar existing protocols. The mutual authentication service between all the authentication entities is achieved. The MCAP supports a complete anonymity service by dynamically changing the encrypted value of (ACI) in an authentication data request message. The true identity of the ATM card cannot be discovered by an attacker eavesdropping over the radio access link interface. Consequently, this offers protection against the personalization attack. MCAP can also achieve the non-repudiation security property since authentication messages contain unique elements based on unique secret keys. For each authentication message there is a unique value and this value can be considered as a user signature. In general the MCAP protocol is resistant against the known attacks of the current authentication protocols. It is also flexible and easy-to-use of users and foremost it doesn't require changing the current ATM system entities infrastructure.

Acknowledgment

We thank all members of Computer Information System Department, Al jouf University, for their support. This work was sponsored by Al jouf University under Grant (141\33).

This work was supported and sponsored in part by Al jouf University under Grant (141\33), Saudi Arabia. Mutual Chain Authentication Protocol for SPAN Transactions in Saudi Arabian Banking.

REFERENCES

[1] Saudi Arabian Monetary Agency. (2013). Ksa financial sector. [Online]. Available: http://www.sama.gov.sa

[2] Bank for International Settlements. (2012). Payment, clearing and settlement systems in Saudi Arabia. [Online]. 2(10), pp. 349-392. Available: http://www.sama.gov.sa

[3] D. Russell. (2011). ATM fraud and security digest. [Online]. Available: http://www.atmsecurity.com

[4] PCI Security Standards Council. (2013). Information supplement: ATM security guidelines. [Online]. Available: http://www.pcisecuritystandards.org

[5] J. McMahon. (2012). Secure your ATMs. [Online]. Available: www.mcafee.com

[6] O. Adeoye, "Evaluating the performance of two-factor authentication solution in the banking sector," *International Journal of Computer Science*, vol. 9, no. 2, pp. 457- 462, 2012.

[7] Cryptomathic A/S (2012). Two factor authentication for banking. [Online]. Available: http://www.cryptomathic.com

[8] S. Bhosale, "Security in e-banking via card less biometric ATMs," *International Journal of Advanced Technology & Engineering Research*, vol. 2, no. 4, pp. 457- 462, 2012.

[9] S. Kurita, K. Komoriya, and R. Uda, "Privacy protection on transfer system of automated teller machine from brute force attack," in *Proc. International Conference on Advanced Information Networking and Applications Workshops*, IEEE computer society, 2012, pp. 72-78.

[10] A. Duvey, D. Goyal, and N. Hemrajani, "A reliable ATM protocol and comparative analysis on various parameters with other ATM protocols," *International Journal of Communication and Computer Technologies*, vol. 1, no. 6, pp. 192-197, 2013.

[11] K. Lavanya and C. Raju, "A comparative study on ATM Security with multimodal biometric system," *International Journal of Computer Science & Engineering Technology (IJCSET)*, vol. 4, no. 6, pp. 808-812, 2013.

[12] F. Hossian, A. Nawaz, and K. Grihan, "Biometric authentication scheme for ATM banking system using energy efficient AES processor," *International Journal of Information and Computer Science*, vol. 2, no. 4, pp. 57-63, 2013.

[13] R. Petrlic, "Automated Teller Machine (ATM) frauds in Nigeria: The way out," *Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 829 – 834, 2011.

[14] S. Sood, "An improved and secure smart card based dynamic identity authentication protocol," *International Journal of Network Security*, vol. 9, no. 1, pp. 39-46, 2012.

[15] U. Singh, M. Pathak, R. Malhotra, and M. Chauhan, "Secure communication protocol for ATM using TLS handshake," *Journal of Engineering Research and Applications (IJERA)*, vol. 2, no. 2, pp. 838-948, 2012.

[16] S. Han, W. Liu, and E. Chang, "Deniable authentication protocol resisting man-in-the-middle attack," *International Journal of Computer, Information Science and Engineering*, vol. 3, no. 3, pp. 696-699, 2007.

[17] C. Raphael and W. Phan. (2003). Attacks on ATM authentication protocols proposed at WEC2002. [Online]. Available: http://citeseerx.ist.psu.edu.

[18] J. A. Saraireh, M. A. Saraireh, S. A. Saraireh, and M. A. Nabhan, "Formal analysis of a novel mutual authentication and key agreement protocol," *Journal of Computer Science & Technology*, vol. 11, no. 2, pp. 86-92, 2011.

[19] M. A. Fayoumi and J. A. Saraireh, "An enhancement of authentication protocol and key agreement (AKA) for 3G mobile networks," *International Journal of Security (IJS)*, vol. 5, no. 1, pp. 35-51, 2011.

[20] A. Suneel, S. Sridevi, and K. Nalini, "Dual security using fingerprint and password in banking system", *International Journal of Review in Electronics & Communication Engineering (IJRECE)*, vol. 3, no. 1, pp. 64-68, 2013.

[21] L. Mohammed, "Use of biometrics to tackle ATM fraud," in *Proc. 2010 International Conference on Business and Economics Research*, vol. 1, 2011.

[22] F. Han, J. Hu, X. Yu, Y. Feng, and J. Zhou, "A novel hybrid crypto-biometric authentication scheme for ATM based banking applications," *Advances in Biometrics*, pp. 675-681, 2005.

[23] S. Oko and J. Oruh, "Enhanced ATM security system using biometrics," *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 3, pp. 352-357, 2012.

[24] A. Ndife, E. fesinachi, A. Okolibe, and D. Nnanna, "An enhanced technique in ATM risk reduction using automated biometrics fingerprint in Nigeria," *International Journal of Scientific Engineering and Technology*, vol. 2, no. 11, pp. 132-138, 2013.

[25] W. Stallings, *Cryptography and Network Security*, 4th ed, *Perason Education*, 2010.

S. I. Nashwan is an assistant professor of computer science at the Department of Computer Science at the University of Al jouf, Saudi Arabia. He earned his BS degree from the College of Science, Ala'zhar University, Palestine, in 2001. He holds a master degree in computer science from the University of Jordan, Jordan, in 2003. In 2009, he received his PhD degree in computer science from the Anglia Ruskin University, United Kingdom and his PhD title was "Performance Analysis of a new Dynamic Authentication Protocol "DAKA" of 3G Mobile Systems based on a novel Cryptography Algorithm "Anglia"". Dr. Nashwan is currently the head of Computer Information System Department at the Al jouf University. He was a member of Telecommunications research Group (TERG) at Anglia Ruskin University, UK, in (2004 – 2009). He has published several papers in the area of authentication protocol, recovery techniques and mobility management.

B. M. Alshammari is an assistant professor of software engineering at the Department of Information Technology at the University of Al jouf, Saudi Arabia. He earned his BS degree from the School of Information Technology, University of Canberra, Australia. He holds a master degree in computer and communications engineering from the Queensland University of Technology, Australia. He earned his PhD in 2012 in Software Security Engineering from the Queensland University of Technology and his PhD title was "Quality Metrics for Assessing Security-Critical Computer Programs". He is currently the acting dean of Admission and Registration at the University of Al jouf. He obtained a number of prizes including a scholarship to study in Australia and the dean of Engineering prize for achieving a GPA of 7 out of 7 in the second semester of his master's degree. He has published several papers in the area of software security, software metrics and information security.