An Approach to Authenticate Magnetic Stripe Bank Card Transactions at POS terminals

Kishor Krishnan Nair
Council for Scientific and Industrial Research (CSIR)
Pretoria
South Africa
knair@csir.co.za

Albert Helberg
North-West University
Potchefstroom Campus
South Africa

Johannes van der Merwe
Council for Scientific and Industrial Research (CSIR)
Pretoria
South Africa

Abstract— **Magnetic stripe card technology has been deployed for more than six decades worldwide and is extensively used in banking. Data embedded in them are often relied upon as a benchmark for user authentication. As such reliance is placed upon them, it is surprising that they do not incorporate stringent security features and therefore attract the attention of criminals who compromise magnetic stripe cards for their illegal gain. Bank cards using magnetic stripe technology are being increasingly cloned or skimmed. Global statistics show that a fraudulent card transaction occurs every eight seconds and that cloning is the principal card fraud, which makes up approximately 37% of overall financial losses. Cloned magnetic stripe bank cards are extensively used at POS terminals and ATMs by criminals. POS terminals are one of the most commonly used payment transaction systems around the world. At the present moment, it is only the signature and PIN that prove the ownership of a magnetic stripe bank card. Even though chip cards are introduced as an extra security mechanism to avoid fraud, the fact that criminals can deliberately damage the chip and force the transaction to fallback to magnetic stripe defeats its intended security purpose. The result of all this fraud is that the original cardholders lose money unknowingly from their bank accounts. One way of enforcing a better security in POS terminals is by incorporating a biometric authentication system, preferably a Fingerprint Authentication System (FAS). This is due to the advantages and convenience that it offers above the other biometric counterparts. Although an FAS can prove the true ownership of a magnetic stripe bank card and can authenticate the transaction using it, this study recognizes existing vulnerabilities pertinent to FAS and biometric authentication systems in general. Hence, the usage of the conventional FAS may lead to severe security vulnerabilities. An FAS with robust security and acceptable recognition performance, at the present moment in time remains unclear and the development of such a system is vital. Thus, the proposal for a secured FAS is put forward to authenticate the transactions performed using magnetic stripe bank cards at POS terminals. The key underlying concept of the proposed system is a unique *One Time Template* which will be valid only for a single transaction session. The proposed FAS will be further evaluated, and criticized in order to illustrate the value added to this study.**

Keywords— authentication, BAS, biometrics, FAS, fingerprint, OTT, POS, PFAS

I. INTRODUCTION

Magnetic stripe card technology, after more than six decades of its successful inception is still widely used in many parts of the world. The banking industry is the primary stakeholder of this technology, which uses it to facilitate the transactions of its account holders. Card cloning is the foremost crime performed on magnetic stripe bank cards and has grown as an epidemic. A study conducted by the Automated Transfer Machine (ATM) Industry Association in the late 2015 raised alarming figures globally as the financial losses due to this fraud exceeds $2 billion a year [1]. The cost of a Point-of-Sale (POS) and ATM skimming on an average is estimated at approximately $50,000 [1]. Considering the heavy financial losses globally due to card cloning, it is highly essential to have an extra security mechanism to address it.

POS terminals, where customer credit or debit cards are swiped for payment, are one of the most frequently used E-payment systems in the developed world [2]. They are used in face-to-face' transactions, where by a merchant swipes a customer's magnetic stripe bank card or key-in payment information and the terminal facilitates the rest of the transaction-processing. Since payments through magnetic stripe bank cards in major businesses such as retail, health-care, restaurants and supermarkets are facilitated through POS terminals, it is vital to identify and prevent the transactions using cloned cards. The main motivations to conduct this study is due to the following core issues or concerns that still remain as a question mark among the banking industry, payment card manufacturers, and card holders. The key motivations are formulated in what follows.

- *Increase in card cloning:* Card cloning or skimming can be described as a process whereby a genuine bank card's magnetic stripe data is copied on to a fake card. The card is swiped through a cloning or skimming device analogous to a magnetic stripe reader on a POS terminal. POS terminals and ATMs are not able to differentiate between a cloned card and the original as the data on both magnetic stripe cards are

identical. Card cloning is increasing heavily in virtually in all major cities of the world, and it has become an international problem [3]. The impact of card cloning is substantial for all stake holders involved in payment systems, and it challenges its integrity. Furthermore, it directly affects industry relationships, merchant behaviors, consumer and employee trust.

➢ *Chip card abuse:* Introduction of chip card technology has undoubtedly helped to alleviate security issues associated with magnetic stripe bank cards. Chip cards are standardised based on the Europay, MasterCard, Visa (EMV) specifications [4]. Although EMV chip cards, to some extent, alleviated security issues associated with an E-payment transaction, criminals have found new ways to hinder the chip card security. One scenario is that criminals clone EMV chip card and damages or disable the chip. So when the cloned chip card is processed at a POS terminal, the transaction will fallback to magnetic stripe and hence will proceed as a normal magnetic stripe transaction. Thus, in effect, the extra security provided by the EMV chip card is nullified.

➢ *Loss of card holder's money:* Financial losses of card holders occurring as a result of card cloning crimes are very high. This attributes to billions of dollars; considering the huge volume of transactions happening every day using payment cards. Retailers worldwide experience $580.5 million in card fraud losses and spend $6.47 billion annually on fraud prevention [5]. According to the 2015 Nilson Report[1], the annual global financial losses due to credit card and debit card fraud equate to $11.2 billion [5]. Millions of card holders worldwide are upset due to card cloning crime and there are a lot of incidences happening every day where the bank accounts of card holders are drained.

➢ *Banks reluctant to pay victims of card cloning:* Banks in majority of the cases are unwilling to admit that their systems could be at fault, and hence refuses to reimburse victims of what is arguably a fraud. As the financial crisis impacts yearly turn over, the banking industry is progressively hesitant to compensate customers who have had the money illegally withdrawn from their bank accounts [6].

➢ *Card holder verification not performed:* Card holder verification is a method which is used to authenticate the card holder and is known as Card holder Verification Method (CVM). The authenticity of card holder at the moment is verified using the following methods.

○ A POS terminal can request card holder's Personal Identification Number (PIN) for card holder authentication before proceeding with a transaction. Although this security mechanism is in place, majority of POS terminal applications in the field complete a transaction without performing PIN authentication.

○ Card holder's signature on the card can be used for authentication purposes. A merchant can compare the signature on the card with the signature on a sale slip, to perform the card holder verification. Since the majority of merchants do not perform authentication of the card holder through signature verification, criminals benefit. Moreover, signature on a newly cloned card can be manipulated by the criminal to match his or her signature. Hence signature verification itself is vulnerable.

○ A merchant can determine whether the card holder is a male or a female by looking at the card holder's name field embedded in the card. In majority of the cases, nobody reads the card holder's name, and it leads to another security vulnerability.

The motivational factors that are discussed in this section clearly indicate that the existing authentication mechanisms are not able to establish a 100% ownership of a person who is performing the transaction and thus fails to bind a transaction to a payment card. As the transactions are sensitive which involves money, precious card holder information, and critical financial data, it is of paramount importance to identify the true ownership of the card holder who is performing the transaction. In the current POS transaction framework, a person who uses a cloned magnetic stripe bank card, knowing the PIN can circumvent the authentication mechanism. Biometric authentication mechanisms are capable of establishing the true ownership of the person who is using the card. Therefore, it is a clear that a strong biometric authentication mechanism must be combined in POS terminals to achieve the expected level of security. Thus, it is highly essential to incorporate a robust fingerprint biometric authentication mechanism in POS terminals to identify and prevent the authentication of transactions using cloned magnetic stripe bank cards. The biometric authentication incorporated must be strong enough to address the card cloning vulnerability and at the same time must not lead to additional vulnerabilities.

At present, the only legally acceptable, fully automated, and mature biometric technique is the fingerprint identification technique, which has been thoroughly researched, used and accepted in forensics since the early 1970s [7]. Currently, the world market for biometric systems is estimated at $112 million and Fingerprint Authentication Systems (FASs) alone account for approximately $100 million [7]. FAS among the others is the most popular and widely used biometric system [8]. FASs for civilian applications and physical access control are growing at a rapid rate [7]. The authentication in FAS basically involves, presenting a fingerprint for query, comparing the presented fingerprint sample to a stored template and determining whether the individual has made a

[1] Nilson Report is a leading publication covering payment system statistics worldwide.

legitimate claim. Even though, the FAS can enhance user convenience and reinforce security, it is also susceptible to various types of threats that are inherent to the biometric security systems in general. They are elaborated as follows [9]:

1. Fingerprints are authentic but are not disclosed and can be easily recorded, replayed, and abused without user's consent [8]. There are numerous instances where artificial fingerprints such as gummy fingers have been used to circumvent security systems [9]

2. Fingerprints cannot be revoked or canceled, passwords and PINs can be reset if compromised. Fingerprints are permanently associated with the user and cannot be revoked if compromised [10]. This also means that if it is compromised in one application, essentially in any application where that finger template was used would be compromised. Although it is possible to enroll multiple fingerprints, there is still a limited choice of fingers to choose from.

3. Cross-matching is used to trace individuals without their consent [11]. Since the finger template might be used in various applications and locations, the user can potentially be tracked if organizations collude and share their respective biometric databases. The fact that a biometric remains the same presents a privacy concern.

Considering all these factors, this study attempts to investigate and incorporate a novel FAS, which can identify and prevent the transactions performed using cloned magnetic stripe bank cards in POS terminals. The proposed solution will be based on a unique finger template of the card owner for each transaction session. The current work is structured as follows: Section II focuses on the existing approaches to mitigate card cloning, analyses it, and identifies the need for a new approach. Section III conceptualizes the Proposed Fingerprint Authentication System (PFAS). Section IV evaluates the PFAS using a standard protocol verification tool known as ProVerif. Section V looks into the scope for future work and conclusions.

II. EXISTING APPROACHES TO MITIGATE CARD CLONING

The following subsections discuss the existing approaches that are in place to mitigate card cloning and analyses their effectiveness.

A. Migration from magnetic stripe bank cards to smart cards: Migration implies the phasing out of the magnetic stripe bank cards that are in use today and reissuing all existing customers with smart cards. There are more than 3 billion magnetic stripe bank cards in use around the world today and this is the real challenge in the migration, and it is less likely that it is going to happen any time soon [12].

B. Diebold's ATM security protection suite: This product consists of anti-cloning packages coupled with monitoring services to provide effective countermeasures against card cloning. It facilitates five levels of protection to guard against the sophisticated card cloning attacks, and the financial institutions are provided with an option based upon the level of protection that they need [13].

C. MagnePrint®: MagnePrint® is a dynamic card authentication technology that determines the originality of the card based on the unique physical properties of the magnetic stripe.

D. PCI DSS compliance: PCI DSS stands for Payment Card Industry Data Security Standards. Security mechanisms that are generic to the financial transactions are implemented as according to the standards mandated by the PCI DSS council [14]. The following paragraphs will be conducting a qualitative comparative study of each solution.

Although smart card seems a viable solution, the drawback is that, it costs about 100 times more than magnetic stripe card [12]. In addition, a large investment has been made in the current magnetic stripe card system and the payment terminals. It is therefore, unlikely that the existing payment infrastructures will be replaced in a short time. Another issue as pointed out in the previous section is that, the criminals clone the magnetic stripe data of the smart cards and damages or disable the chip in the cloned smart cards purposefully. So when the cloned smart cards are processed at the POS terminals, the transactions will fallback to magnetic stripe. In effect, the transaction will be processed as a normal magnetic stripe transaction and the smart card security mechanisms are bypassed. To make the MagnePrint® solution to work practically in the field; the entire card processing devices and issuers must agree to read, record, and share their card's magnetic data signatures. It is also a mandatory requirement that all merchants must agree to use POS terminals that have the ability to read the magnetic signature of the card. These requirements add extra overheads, cost, and a lot of inconvenience; there by practically making it an infeasible solution.

The solution provided by the Diebold is only intended for ATMs and does not address the card cloning issue in POS terminals. The PCI DSS council enforces the financial institutions and payment networks to implement the requirements which are proposed in its standards. It has been observed that many merchants, acquirers, and service providers are not conforming to the PCI DSS standards. As reported by Visa, only 22% percent of its largest merchants were compliant, not to mention smaller merchants with tight budgets and resources [15]. The payment card fraud continues to evolve, and each countermeasure forces the criminals to become more sophisticated. There is as yet no clear and consistent set of industry-wide security standards for protection of payment systems. The root cause behind the transaction security issue is the remote nature of the transaction. In this transaction scenario, the individual is at the remote end of a communication channel and identifiable only by weak security tokens that they have such as a password or a PIN. Payment systems should be capable of achieving robust user authentication, especially in an online environment. This

can be achieved by the usage of biometric techniques, which will add top class security to the payment card transactions.

III. CONECPTUALIZATION OF THE PFAS

In the PFAS, the fingerprint authentication phase will biometrically authenticate if the card is belonging to the correct person. If the authentication is successful, then it is concluded that, it is the owner of the card who is performing the transaction and therefore it is genuine. On the contrary, if the authentication fails, then it is ascertained that the card is not belonging to its owner and therefore it is very much possible that the transaction could be performed using a cloned card. Hence the POS terminal will prevent the transaction to proceed further. The key objectives set for the PFAS are as follows:

- Preserve the privacy and security of template data.
- Mutual authentication.
- Be resilient to the compromise of the template itself.
- Support revocation of the template, in case it gets compromised.
- Be resilient to replay attacks so that the replay of the template does not result in a successful authentication.

The PFAS is conceptualised based on the above key objectives, and are explained through the following subsections.

A. *Proposed security model*

To solve the research problem and to achieve the objectives of the PFAS, this research proposes a security model that is based upon the principles of Biohashing and One-Time Password (OTP) scheme. The key concept behind the Biohashing is to apply transformation function on a biometric feature to transform it into another format [16]. The OTP scheme is a well-known authentication technique in electronic transactions, where an OTP is generated for authenticating a particular transaction session [17]. The PIN or password generated can be used only once and hence a robust security can be achieved. Thus, the proposal is to derive an unpredictable, one-time finger template by inheriting the principles of Biohashing and OTP scheme. The *One Time Template* (OTT) will be generated based on the parameters that are pertinent to the current transaction session. During the authentication phase, the OTT derived for authenticating the user in the POS is matched against the OTT at the Biometric Authentication Server (BAS), and the decision is taken accordingly.

B. *Authentication process*

The authentication process between the POS and the BAS is presented as a sequence of steps in what follows.

Step 1: During the enrollment phase, the finger template of the user, along with a set of key user attributes is registered in the BAS.

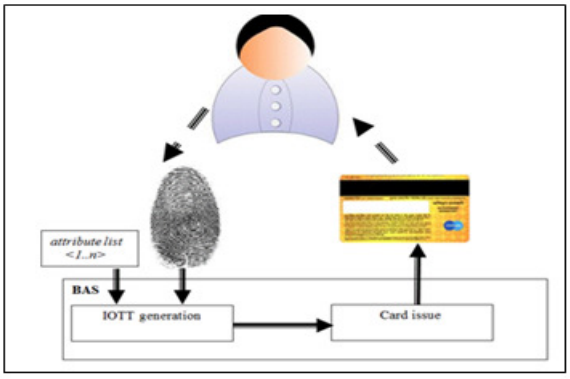

Figure 1. Enrollment and card issue process

In the current security model, the attribute list is limited to 8 entries as it is adequate to generate the expected level of security, and at the same time it saves the average time to enroll each user. The enrollment and card issue process are illustrated in Figure 1.

Step 2: The BAS is equipped with an intermediate OTT generation module. This module takes as input the extracted finger template and the attribute list. The user's *Intermediate One Time Templates* (IOTTs) are subsequently generated for each *Transaction Number* (TSN), based on the *Biometric Keys* (BKs) derived from the attribute list captured in Step 1. The enrollment and card issue process is complete at this stage. The TSN, BK and the corresponding IOTT list are mapped to the user's Primary Account Number (PAN) in the IOTT database, as illustrated in Table 1, where xxxxxxxxxxxxxxx is the 16 digit PAN corresponding to the user. The value of *n* in Table 1 is limited to 73200, which this study considers as ample from the following hypothesis. If a user performs 50 transactions per day, and continuously throughout the year (taking leap years into consideration) for a period of 4 years, then the user will be performing a maximum of 73200 transactions, which is considered to be more than is expected. A general business rule and norm in the banking industry is to replace bank cards after the specific expiry date, which is normally after 3 or 4 years [18]. This is essentially because of card limitations such as maximum transactions that can be performed during the lifetime of a card, wear and tear of the card, and to mitigate card fraud [18]. Note that in this approach, only the transformed IOTTs are stored and the original user templates are never stored in the BAS.

Table 1. IOTT database

PAN: xxxxxxxxxxxxxxx		
TSN	BK	IOTT
TSN1	*BK1*	*IOTT1*
TSN2	*BK2*	*IOTT2*
...	...	...
TSNn	*BKn*	*IOTTn*

Step 3: On the client side, the magnetic card swipe in the POS triggers transaction processing. The POS then captures the PAN, the current date stamp, and the time stamp. These fields are subsequently encapsulated in an online logon request message, which is sent to the BAS.

Step 4: The BAS on receiving the logon request, queries its user template database against the PAN. The appropriate BK that is pertinent to the transaction and the TSN is retrieved.

They are then assembled in a logon reply message, and transmitted to the client. This is illustrated in Figure 3. Note that the TSN gets incremented after every authentication attempt from the client.

Step 5: After sending the logon reply, the BAS generates an OTT, which is used for authenticating the current transaction session. If this was the first transaction attempt for the client, it implies that *TSN1* and *BK1* were used in deriving *IOTT1*. The *IOTT1* is subsequently transformed using the current date stamp and time stamp received in the logon request to derive the actual OTT. In this case, *OTT1* will be generated. The role of the current date stamp and time stamp as extra security salts in the protocol is to strengthen the security of the generated OTT, and to add an element of unpredictability in future transactions. The OTT generation process in the BAS is illustrated in Figure 2.

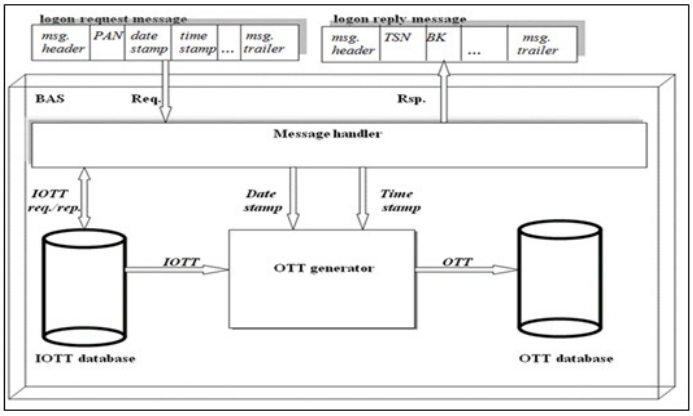

Figure 2. OTT generation in the BAS

Step 6: The POS, on receiving the logon reply, captures the finger template of the user. It then follows the transformation process based on the *TSN* and the *BK* that was received from the BAS in the logon reply. The IOTT will be generated and transformed using the current date stamp, and the time stamp to generate the actual OTT. In this case, *OTT1* will be derived from *IOTT1* and is sent as an online authentication request to the BAS. This process is illustrated as in Figure 3.

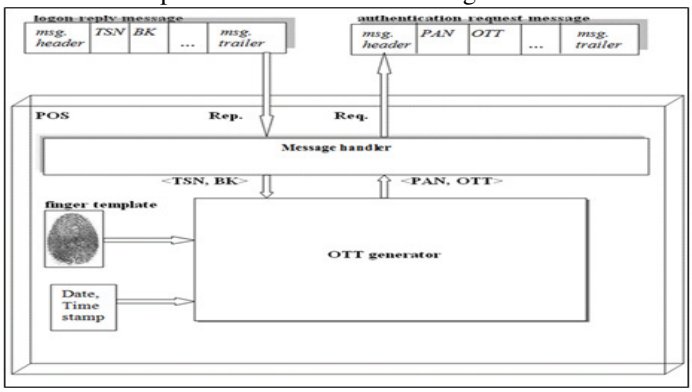

Figure 3. OTT generation in the POS

Step 7: The BAS, on receiving the authentication message compares the OTT generated from the POS against the OTT generated at the BAS and decides if the OTTs match, based on the decision threshold set in the BAS. The status is sent down to the client as an authentication reply. After sending the authentication reply, the BAS deletes the OTT for that transaction session.

Step 8: The POS on receiving the authentication reply, checks the response code. If the response code is a success, the POS proceeds with the rest of the transaction processing as normal. If the response code is a failure, then the transaction processing is terminated at this stage.

IV. EVALUATION OF THE PFAS

The research within the field of security protocol verification is a productive area because security protocols are often prone to errors, and it is not easy to identify errors through manual verification procedures. The well-known automatic tools, such as ProVerif, Capser and Avispa are most commonly used for evaluating the security protocols [19]. ProVerif is well-known for modeling and analysing security protocols [19]. Furthermore, its applicability has been widely validated and has also been extensively used in numerous case studies of security protocols.

ProVerif was developed by Bruno Blanchet and is dedicated to proving secrecy, authenticity, and other properties of security protocols [20]. It accepts as input a set of queries and outputs true or false for each query. The queries are first translated to a set of clauses [20]. This will yield an abstract representation of the protocol, and ultimately ProVerif aims to resolve these clauses. To ensure that the PFAS provides the appropriate level of security and the objectives that it upholds in addressing the research problem, the ProVerif model will be used in the verification. The main block diagram of the PFAS is presented in Figure 4. The current model incorporates a *U Process (UP)*, *POS Process (PP),* and a *BAS Process (BP)*. The communication between the processes is based on the key events or messages listed in Table 2. The *UP* is responsible for all activities pertaining to the user. The *PP* interfaces with the *UP* and *BP* in facilitating the transaction process. The *BP* is primarily responsible for the course of actions involved in authenticating the requests from the *PP*. Scripts were developed in the ProVerif grammar to evaluate the security objectives in terms of *UP, PP,* and *BP* process communications that simulates the PFAS.

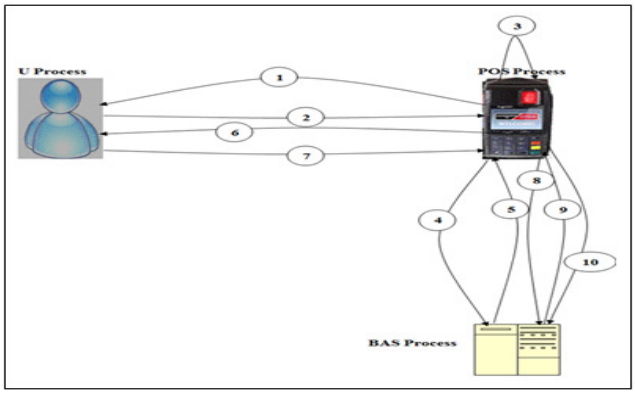

Figure 4. ProVerif model of the PFAS

Each of the security objective is analysed in the following subsections. It should be noted that, although each of the objectives are addressed separately, they are interdependent in

many ways; as a result, the discussions of the objectives may overlap to some degree. In order to validate whether the model meets its intended objectives, various attacks on the PFAS are generated in the scripts corresponding to each process. The objectives are analysed in terms of the *event* and *query commands*. The *event command* is used to launch an event when a specific action is executed, whereas the *query command* is used to prompt ProVerif to validate the correctness of the sequence of specified events. If it is determined that the sequence is not correct, ProVerif declares that an attack has been identified. As with any security measurement tool, ProVerif can validate only generic security objectives. Therefore, the objectives that are specific to the PFAS will be analysed based on logical propositions and facts.

Table 2. Label to Event Message Mappings

Label	Event
1	PresentCard
2	CardPresented
3	CardSwiped
4	LogonRequest
5	LogonResponse
6	PresentFingerPrint
7	FingerPrintPresented
8	AuthenticationRequest
9	AuthenticationResponse
10	AuthenticationStatusUpdate

1. *Privacy and security:* The privacy and security of the finger template data are of utmost importance to the PFAS, as the compromise of the template data will be of permanent nature. Security implies that data is readily available to authorized people and is unavailable to unauthorised people [21]. Privacy reduces the pool of authorised people to those individuals who have a valid need to access the data. There is a truism that "*You can have security without privacy, but you cannot have privacy without security*" [22]. This implies that the confidentiality of template data must be protected to ensure privacy, and that security mechanisms are required in order to provide this protection. In the PFAS model, the following queries are executed.

- *query attacker (MSCD)*
- *query attacker (FPPresented)*

```
--Query attacker(MSCD[]) Completing...
Starting query  attacker(MSCD[])
RESULT attacker(MSCD[]) is false.
--Query attacker(FPPresented[]) Completing...
Starting query  attacker(FPPresented[])
RESULT  attacker(FPPresented[]) is false.
```

Figure 5. Test result 1

The results of the queries *attacker (MSCD)* and *attacker (FPPresented)* are *false*, which imply that they are not attacks. This indicates that the magnetic stripe card presented during the transaction is genuine. If the results of the queries were *true*, then it would have implied that the queries were attacks, and that the magnetic stripe card presented during the transaction was a cloned card. Hence, the results reveal that the privacy and security property are kept intact in the PFAS, and that it does not lead to a compromise.

2. *Mutual Authentication:* Authentication occurs after identification and before authorization. It validates the authenticity of the identity declared during the identification phase. Mutual authentication implies the act of two parties thoroughly authenticating each other [22]. In the PFAS, the processes authenticate each other by using events to ascertain the mutual authentication. Hence, the relevant queries were written to test the processes in order to establish whether one event is not executed before another event or a group of events, and whether the mutual authentication was carried out as expected. The following queries were executed in the *UP*. The test results of these queries are presented in Figure 6.

- *query event (evAuthenticationResponseSuccess) ==> event (evPresentFP) && event (evPresentMSC)*
- *query event (evAuthenticationFailure) ==> event (evPresentFP) && event (evPresentMSC)*

```
RESULT event(evAuthenticationResponseSuccess) ==>
        (event(evPresentFP) && event(evPresentMSC)) is true.
RESULT event(evAuthenticationFailure) ==> (event(evPresentFP) &&
        event(evPresentMSC)) cannot be proved.
```

Figure 6. Test result 2

The results of the queries reveal that mutual authentication is successfully carried out in the *UP*. The following queries were executed in the *PP*.

- *query event (evLogonResponseSuccess) ==> event (evCardSwiped) && event (evMSCPresented)*
- *query event (evTransactionDeclined) ==> event (evLogonResponseFailure) && event (evCardSwiped) && event (evMSCPresented)*
- *query event (evTransactionContinue) ==> event (evAuthenticationResponseSuccess) && event (evLogonResponseSuccess) && event (evFPPresented) && event (evCardSwiped) && event (evMSCPresented)*
- *query event (evTransactionDeclined) ==> event (evAuthenticationFailure) && event (evLogonResponseSuccess) &&event (evFPPresented) && event (evCardSwiped) && event (evMSCPresented)*

The test results of these queries are presented in Figure 7 and they reveal that the mutual authentication is successfully carried out in the *PP*. The following queries were executed in the *BP*.

- *query event (evLogonResponseSuccess) ==> event (evLogonRequest)*
- *query event (evLogonResponseFailure) ==> event (evLogonRequest)*
- *query event (evAuthenticationResponseSuccess) ==> event (evLogonRequest) && event (evLogonResponseSuccess) && event (evAuthenticationRequest)*
- *query event (evAuthenticationFailure) ==> event (evLogonRequest) && event (evLogonResponseSuccess) && event (evAuthenticationRequest)*

The test results of these queries are presented in Figure 8. The results of the queries reveal that mutual authentication is successfully carried out in the *BP*. Since all the processes successfully carry out this security property, it is established that this security property remains intact in the PFAS.

```
vent(evCardSwiped) && event(evMSCPresented))RESULT
vent(evTransactionDeclined) ==> (event(evAuthenticationFailure) &&
vent(evLogonResponseSuccess) && event(evFPPresented) &&
vent(evCardSwiped) && event(evMSCPresented)) is true.-- Query
RESULT event(evTransactionContinue) ==>
(event(evAuthenticationResponseSuccess) &&
vent(evLogonResponseSuccess) && event(evFPPresented) &&
vent(evCardSwiped) && event(evMSCPresented)) is true.
RESULT event(evTransactionDeclined) ==>
(event(evLogonResponseFailure) && event(evCardSwipped) &&
vent(evMSCPresented)) is true.-- Query event(evLogonResponseSuccess)
```

Figure 7. Test result 3

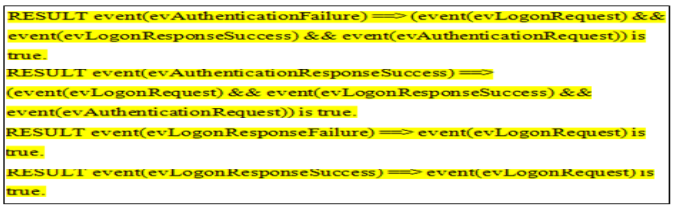

Figure 8. Test result 4

3. *Resilience to compromise of finger templates:* The term "compromise" is loosely used in cryptography to imply that a password or a token has been exposed [22]. In biometrics, it has a different meaning and consists of three components. Firstly, the attacker has to possess a reproduction of the biometric template. Secondly, in order to make it practical, the attacker must have the knowledge and technology to be able to use it in a biometric authentication system. Thirdly, the attacker must be capable of mitigating any countermeasures that are applied to prevent its use [22]. In the PFAS, a unique OTT is generated in the POS and the BAS during each authentication session. As the name implies, an OTT can be used only once. Furthermore, the original finger template is not stored anywhere, and hence the current scheme is resilient to the compromise of the original finger template data.

4. *Revocation support:* According to ITU-T X.811[2], the definition of revocation is the "permanent invalidation of verification and authentication information" [23]. In the PFAS, even if an OTT is compromised, it is still revocable and replaceable. The original template of the user never leaves the POS or gets stored in the BAS. This offers more significant benefits to the users in terms of privacy and security. After the necessary transformation, the finger template is intentionally distorted to an IOTT and then to an OTT. These new versions of the finger template are secure, as the original fingerprint pattern cannot be reverse engineered from the OTT used during the authentication phase. They are also cancelable, as a totally different pattern or code can be generated using the transformation process. This is done by using a different finger template of the user or a different combination of attributes captured during the re-enrollment. Using this technique, one or two fingerprints can be mapped to a total of *n* different virtual IOTTs, thereby fulfilling the objective of the revocation support in the case of a compromised template.

5. *Replay attack:* A replay attack is a two or three-stage process; first intercepting or copying the sensor transmission, then possibly modifying the data, and finally replaying the signal [24]. In certain replay attacks, a false data stream may be injected between the sensor and the processing system. In most cases, this involves some physical tampering with the system [24]. If the true fingerprint is disclosed in the conventional FAS protocol, then the FAS is vulnerable to a replay attack. In the worst case, the same fingerprint could be used to illegally gain access to multiple databases, and database cross matching could be carried out to gather business intelligence [24]. The enrollment entity stores neither the original finger template nor the users' attribute list during the fingerprint enrollment process. By not storing this information, the possibility of future replay attacks is eliminated. In addition, the PFAS generates an OTT for each authentication session. Hence, even if one OTT template in one authentication session is compromised, it cannot be reused to launch a replay attack for future authentication sessions as the OTT is unique for each authentication attempt. As a result, the replay of the template does not result in successful authentication in the PFAS.

[2] ITU-T X.811 is the specification for an open systems interconnection authentication framework.

V. FUTURE WORK AND CONCLUSIONS

Although this research achieved its objectives, there still remains a potential for improvement. The focus of this study was on alleviating the major vulnerabilities based on the key objectives identified. A further research can well be conducted to address the compromise of the original finger templates at the sensing device or on the channel between the sensing device (scanner) and the POS terminal. The IOTT/OTT generation process and storage in the PFAS can also be improved as millions of users with billions of transactions occur on a daily basis. Hence, the IOTT/OTT could only be generated dynamically on demand to address the scalability constraints. The scalability aspects can be studied further, depending on the use case where the proposed work needs to be deployed. Further study can be conducted to understand the interoperability aspects between the different fingerprint scanners. This is to understand and address cases such as, whether the finger template enrolled using the fingerprint scanner of manufacturer X will match against the finger template presented at the fingerprint scanner of manufacturer Y, and vice versa.

REFERENCES

[1] K. Piero and J. Finefrock, "Diebold Stops ATM Fraudsters In Their Tracks With World's Most Secure Anti-Skimming Card Reader," 2014.http://news.diebold.com/press-releases/diebold-stops-atm-fraudsters-in-their-tracks-with-worlds-most-secure-anti-skimming-card-reader.htm

[2] M. Bond, O. Choudary, S.J. Murdoch, S. Skorobogatov, and R. Anderson, "Chip and Skim: cloning EMV cards with the pre-play attack," in Proc. of the IEEE Symposium on Security and Privacy, SP, 18-21 May, 2014, San Jose, CA, IEEE , 2014, ISSN. 1081-6011, pp. 49-64, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6956556

[3] H. Guo and B. Jin, "Forensic Analysis of Skimming Devices for Credit Fraud Detection," in Proc. of the 2nd IEEE International Conference on Information and Financial Engineering, ICIFE, 17-19 Sep., 2010, Chongqing. IEEE, 2014, ISBN. 978-1-4244-6927-7, pp. 542-546, http:// ieeexplore.ieee.org/xpl/ articleDetails.jsp? arnumber=5609418

[4] U.G. Ceipidor, C.M. Medaglia, A. Marino, S. Sposato, and A. Maroni, "KerNees A protocol for mutual authentication between NFC phones and POS terminals for

secure payment transactions," in Proc. of the 9th Int. Conf. on Information Security and Cryptology, ISCISC, 13-14 Sep., 2012, Tabriz. IEEE, 2012, ISBN. 978-1-4673-2387-1, pp. 1-7. http://ieeexplore.ieee.org/xpl/ articleDetails.jsp? arnumber=6408203
[5] M.K. Mishra and R. Dash, "A Comparative Study of Chebyshev Functional Link Artificial Neural Network, Multi-Layer Perceptron and Decision Tree for Credit Card Fraud Detection," in Proc. of the Int. Conf. on Information Technology, ICIT, 22-24 Dec., 2014, Bhubaneswar. IEEE, 2014, ISBN. 978-1-4799-8083-3, pp. 228-233, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7033327
[6] "Banks reluctant to pay victims of chip-and-PIN fraud," 2010,http://www.timesonline.co.uk/ tol/money/consumer_affairs/article5575295.ece
[7] A.A. Albahdal and T.E. Boult, "Problems and Promises of Using the Cloud and Biometrics," in Proc. of the 11th International Conference on Information Technology: New Generations, ITNG, 7-9 Apr., 2014, Las vegas, NV. IEEE, 2014, ISBN. 978-1-4799-3187-3, pp. 293-300, http://ieeexplore. ieee.org/stamp/ stamp.jsp?tp=&arnumber=6822213
[8] A.A. Darwish et al., "Human Authentication using Face and Fingerprint Biometrics," in Proc. of the 2010 2nd Int. Conf. on Computational Intelligence, Communication Systems and Networks (CICSyN), 28-30 Jul. 2010 Liverpool. IEEE,http://ieeexplore.ieee.org/xpl/ articleDetails.jsp? arnumber=5616134
[9]National Institute of Standards and Technology (NIST), 2003. "Face Recognition Vendor Test 2002: Evaluation Report,"http://www.face- rec.org/ vendors/FRVT_2002_Evaluation_Report.pdf
[10]M. Fons et al., "Hardware-Software Co-design of an Automatic Fingerprint Acquisition System," in Proc. of the IEEE Int. Symposium on Industrial Electronics, ISIE 2005 20-23 Jun. 2005. IEEE,http://ieeexplore. ieee.org/xpl/articleDetails.jsp?arnumber=1529081
[11]N. Nishiuchi, H. Soya, "Cancelable Biometric Identification by Combining Biological Data with Artifcats," in Proc. of the 2011 Int. Conf. on Biometrics and Kansei Engineering (ICBAKE), 19-22 Sep. 2011 Takamatsu. IEEE, http://ieeexplore.ieee.org/xpl/ articleDetails.jsp?arnumber=6031251
[12] B. Smyth, M. Ryan, S. Kremer, and M. Kourjieh, "Towards automatic analysis of election verifiability properties," 2009, http://citeseerx. ist.psu.edu/viewdoc/summary?doi=10.1.1.153.5726
[13] S. Kremer, M. Ryan, and B. Smyth, "Election verifiability in electronic voting protocols," in Proc. of the 15th European conference on Research in computer security, ESORICS, 2010, Berlin. ACM DL, ISBN. 3-642-15496-4 978-3-642-15496-6, pp. 389-404, http://dl.acm.org/citation.cfm?id=1888912
[14] M. Backes, M. Maffei, and D. Unruh, "Zero-Knowledge in the Applied Pi-calculus and Automated Verification of the Direct Anonymous Attestation Protocol," in Proc. of the IEEE Symposium on Security and Privacy, SP, 18-22 May, 2008 Oakland, CA. IEEE, 2008, ISBN. 978-0-7695-3168-7, pp. 202-215, http://ieeexplore.ieee.org/ stamp/stamp.jsp?tp=&arnumber=4531154
[15]N.D. Sarier, "Practical Multi-factor Biometric Remote Authentication," in Proc. of the 2010 Fourth IEEE Int. Conf. on Biometrics: Theory Applications and Systems (BTAS), 27-29 Sep. 2010 Washington DC, http:// ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5634541
[16]S. Ding et al., "Protecting Hidden Transmission of Biometrics Using Authentication Watermarking," in Proc. of the 2010 WASE Int. Conf. on Information Engineering (ICIE), 14-15 Aug. 2010 Beidaihe. IEEE, http://ieeexplore. ieee.org/xpl/articleDetails.jsp?arnumber=5571271
[17] O. Ogundele, P. Zavarsky, R. Rahul, and D. Lindskog, "The Implementation of a Full EMV Smartcard for a Point-of-Sale Transaction and its Impact on the PCI DSS," in Proc. of the Int. Conf. on Social Computing: Privacy, Security, Risk and Trust, PASSAT, 3-5 Sep., 2012, Amsterdam. IEEE, 2012, ISBN. 978-1-4673-5638-1, pp. 797-806, http://ieeexplore.ieee.org/xpl/ articleDetails.jsp?arnumber=6406326
[18]L.C. Paul, "The Inductive Approach to Verifying Cryptographic Protocols," 2000, http://www.cl.cam.ac.uk/~lp15/papers/Auth/jcs.pdf
[19] A. Salaiwarakul and M.D. Ryan, "Verification of Integrity and Secrecy Properties of a Biometric Authentication Protocol," 2008, http://www.cs. bham.ac.uk/~mdr/research/papers/pdf/08-biometric.pdf.
[20] B.S. Kurhade and M. Kshirsagar, "Formalization and Analysis of Borda protocol using pi calculus," in Proc. of the Int. Conf. on Pattern Recognition, Informatics and Mobile Engineering, PRIME, 21-22 Feb., 2013, Salem. IEEE, 2013, ISBN.978-1-4673-5843-9, pp. 232-236, http://ieeexplore. ieee.org/xpl/articleDetails.jsp?arnumber=649 6478
[21] K. Nair, A. Helberg, J. Van Der Merwe "Intrusion Detection in Bluetooth Enabled Mobile Phones," in Proc. of the Int. Conf. on Pattern Recognition, Informatics and Mobile Engineering, PRIME, 21-22 Feb., 2013, Salem. IEEE, 2013, ISBN.978-1-4673-5843-9, pp. 232-236, http://ieeexplore. ieee.org/xpl/articleDetails.jsp?arnumber=649
[22] International Committee for Information Technology Standards INCITS , "Study Report on Biometrics in E-Authentication," 2007, https://standards. incits.org/ apps/group_public/download.php/24528/m1070185rev.pdf
[23] "Information Technology– Open Systems Interconnection- Security Frameworks for Open Systems; Authentication Framework", ITU-T Recommendations ITU-T X.811(04/95), 2008, http://www.itu.int/ rec/T-REC-X.811/en
[24] C. Roberts, "Biometric Attack Vectors and Defenses," Journal of Computers & Security, ScienceDirect, 2007. vol. 26, no. 1, doi. 10.1016/j.cose.2006.12.008, pp 14–25, http://www.sciencedirect.com/science/ article/pii/S016740480600215X