ATM Frauds -Preventive Measures and Cost Benefit

Lawan Ahmed Mohammed
King Fahd University of Petroleum and Minerals
HBCC Campus, Hafr Al Batin 31991, Saudi Arabia.
Email: gumel@hbcc.edu.sa

***Abstract* – It is well-known that criminals have many ways of illegally accessing ATM machines to access the account of legitimate users. In this paper, we briefly provide an overview of the possible fraudulent activities that may be perpetrated against ATMs and justify why the use of biometric should be considered as preventive measure. A prototype of biometric ATM was designed and questionnaires were distributed to users for their opinion. Finally, the paper concludes by giving a simple risk and cost benefit analysis for the proposed design.**

Keyword(s): ATM Fraud, Biometrics, Fingerprint Verification, ATM Fraud Countermeasures.

I. INTRODUCTION

An automated teller machine was first introduced in 1960 by City Bank of New York on a trial basis, the concept of this machine was for customers to pay utility bills and get a receipt without a teller [1]. It allows financial institutions to provide their customers with a convenient way, round the clock, to carry out varying transactions which included withdrawal of funds, made deposits, check account balance, and later on included features to allow customers pay bills, etc. ATMs are not only located at banks but also increasing numbers of businesses, especially retailers for both customer convenience and a new revenue stream. A global ATM market forecast research conducted by Retail Banking Research Limited [2] shows that there are 1.8 million ATMs deployed around the world today and the figure is forecast to reach 2.5 million by 2013.

Authentication methods for ATM cards have little changed since their introduction in the 1960's. Typically, the authentication design involves a trusted hardware device (ATM card or token). The card holder's Personal Identification Number (PIN) is usually the only means to verify the identity of the user. However, due to the limitations of such design, an intruder in possession of a user's device can discover the user's PIN with brute force attack. For instance, in a typical four digits PIN, one in every 10,000 users will have the same number. The security limitations of ATM are mostly derived from the security pitfalls of the magnetic media. The data in the magnetic stripe is usually coded using two or three tracks. The standard covering this area is ISO 7811. The technique for writing to the tracks is known as F/2F. The reason is that it is not that difficult and/or expensive to have the equipment to encode magnetic stripes. Fortunately, magnetic stripe weakness has been partly addressed by the introduction of EMV smartcards. Despite security measures, cases of ATM crimes continue to occur globally. Incidents have been reported in Asia-Pacific, the Americas, Africa, Russia and the Middle East. Some examples include are reported in {[3], [4] and [5]}. This paper is organized as follows: the next section briefly discusses different security breaches in ATM system. Section three explained the proposal design. Finally, section four concludes the paper.

II. TYPES OF ATM FRAUDS

In the last few years, there have been many reports of hacking into the electronic ATM system and caused billion dollars of losses in the banking company itself. Oracle attack on authentication protocols and breaches affecting the ATM machine such as cloning of cards and hacking of PIN code have been reported increasingly. Some popular ATM frauds/attacks are explained below in the following subsection.

A. Skimming Attack

This is the most popular breach in ATM transaction. In this ingenious rip-off, lawbreakers are taking advantage of technology to make counterfeit ATM cards by using a skimmer (a card swipe device that reads the information on ATM card). These devices resemble a hand-held credit card scanner and are often fastened in close proximity to or over top of an ATM's factory-installed card reader. When removed from the ATM, a skimmer allows the download of personal data belonging to everyone who used it to swipe an ATM card. A single skimmer can retain information from than 200 ATM cards before being re-used.

B. Card trapping

This involves placing a device directly over or into the ATM card reader slot. In this case, a card is physically captured by the trapping device inside the ATM and the fraudster tries any method to capture the customer‘s PIN. When the customer leaves the ATM without their card, the card is retrieved by the thieves. Typically only one card is lost in each attack. The criminals have to withdraw the whole device each time a card is trapped, although recently a card trapping device has been seen that can stay in place for a period of time and that allows removal of trapped cards without the removal of the device. The most common variant is known as the Lebanese Loop.

C. PIN Cracking

Attacks on customers' PINs have been known to security researchers for years, e.g., [6], [7], [8]. One of the most efficient of these 'PIN cracking' attacks are due to Berkman and Ostrovsky [9]. It explained how the processing system used by banks is open to abuse. One of the attacks targets the translate function in switches - an abuse functions that are used to allow customers to select their PINs online. In either case, the flaws create a means for an attacker to discover PIN codes, for example, those entered by customers while withdrawing cash from an ATM providing they have access to the online PIN verification facility or switching processes. A bank insider could use an existing Hardware Security Module (HSM) to

DOI: 10.5176_2010-2283_1.2.43

reveal the encrypted PIN codes. Even worse, an insider of a third-party Switching provider could attack a bank outside of his territory or even in another continent. Unfortunately, proposals to counter such attacks are almost non-existent other than a few suggestions; for example, maintaining the secrecy (and integrity) of some data elements related to PIN processing (that are considered security insensitive according to current banking standards) such as the 'decimalization table' and 'PIN Verification Values (PVVs)/Offsets' has been emphasized [7], [9].

D. Phishing/Vishing Attack

Phishing scams are designed to entice the user to provide the card number and PIN for their bank card. Typically, an attacker uses email representing them as a bank and claiming that user account information is incomplete, or that the user needs to update their account information to prevent the account from being closed. The user is asked to click on a link and follow the directions provided. The link however is fraudulent and directs the user to a site set up by the attacker and designed to look like the user‘s bank. The site directs the user to input sensitive information such as card numbers and PINs. The information is collected by the thieves and used to create fraudulent cards. Some variants are spear phishing and Rock Phish attacks.

Traditionally, after a successful phishing attack, the criminal would extract the needed information and go onto the online account and remove the victim's bank funds. This has changed for some of the more sophisticated criminals in recent years were instead of looting the victim's account; they go to the check image page, where they take a copy of the victim's check. Many financial institutions are now offering check images as part of their online banking services to their customers. The checks contain the victim's bank account number, signature, address, phone etc. The attacker can either take the copy and make paper counterfeit checks, or take that information and create PayPal accounts or other online payment accounts.

E. ATM Malware

Malware attacks required an insider, such as an ATM technician who has a key to the machine, to place the malware on the ATM. Once that was done, the attackers could insert a control card into the machine's card reader to trigger the malware and give them control of the machine through a custom interface and the ATM's keypad. According to a report in [10] found a Trojan family of malware that infected 20 ATMs in Eastern Europe. The malware lets criminals take over the ATM to steal data, PINs and cash. The malware captures magnetic stripe data and PIN codes from the private memory space of transaction-processing applications installed on a compromised ATM.

F. ATM hacking

Attackers use sophisticated programming techniques to break into websites which reside on a financial institution's network. Using this access, they can access the bank's systems to locate the ATM database and hence collect card information which can be used later to create a clone card. Hacking is also commonly used to describe attacks against card processors and other components of the transaction processing network. Most of the ATM hackings are due to the use of non-secure ATM software.

III. SECURITY MEASURES

As technology advances, as ATM applications become more ubiquitous, as more confidential data is transmitted over the ATM system, as more sensitive transactions are conducted, as more threats breaches are reported, the challenge of securing the system becomes more urgent. Many security services in bank transactions are dependent on authenticating users such as generation of accurate audit trails, non-repudiation in communications, preserving confidentiality and other input validation techniques such as batch totals, format checks, reasonableness checks, and transaction validation. These features only ensure that certain procedures are followed, and cannot tell whether the person with the card and PIN is authorized to use it, they just ensure that the data transmitted follows certain guidelines or protocols that requests such as cash withdrawals are made within reasonable limits, that money is transferred to the proper account, and so forth. Therefore, it is essential to develop stronger authentication and identification measures to stop criminals from committing fraudulent act. One of best security measures against some of the attacks mentioned above is the deployment of biometric in the current ATM system as discussed below.

Biometric Smartcard – A prototype

Biometric identification is utilized to verify a person's identity by measuring digitally certain human characteristics and comparing those measurements with those that have been stored in a template for that same person. Templates can be stored at the biometric device, the institution's database, a user's smart card, or a *Trusted Third Party* service provider's database. There are two major categories of biometric techniques: *physiological* (fingerprint verification, iris analysis, hand geometry-vein patterns, ear recognition, odor detection, DNA pattern analysis and sweat pores analysis), and *behavioral* (handwritten signature verification, keystroke analysis and speech analysis). In [11], it was found that behavior based systems were perceived as less acceptable than those based on physiological characteristics. Of the physiological techniques, the most commonly utilized is that of fingerprint scanning. With biometrics, such fraudulent incidents can be minimized, as an added layer of authentication is now introduced that ensures that even with the correct pin information and in possession of another person's ATM card, the user's biometric features cannot easily be faked. The advantages of this may include: all attributes of the ATM cards will be maintained, counterfeiting attempts are reduced due to enrolment process that verifies identity and captures biometrics, and it will be extremely high secure and excellent user-to-card authentication. These advantages are for the benefit of users as well as system administrators because the problems and costs associated with lost, reissued or temporarily issued can be avoided, thus saving some costs of the system management.

On the negative side, the major risk posed by the use of biometric systems is that a malicious subject may interfere with the communication and intercept the biometric template and use it later to obtain access [12]. Likewise, an attack may be committed by generating a template from a fingerprint obtained from some surface. Although few biometric systems are fast and accurate in terms of low false acceptance rate enough to allow identification (automatically recognizing the user identity), most of current systems are suitable for the verification only, as the false acceptance rate is too high.

The propose design uses a maximum of 8 characters, numbers or mix of the both PIN and fingerprint as verification factors of the authentication process. ACOS smartcards and AET60 BioCARDKey development kit were used in the propose design. In the verification part, the users have to submit the correct PIN DES encrypted current session key to get access to the next level. Users have 3 successful attempts to enter the correct PIN, else the cards will be locked and render it to useless. Lastly, we use the fingerprint as the biometric identifiers as it takes shortest enrollment time. The proposed design involves two phases namely enrollment phase and verification phase. Each of the phases is briefly describe below.

Enrollment - Prior to an individual being identified or verified by a biometric device, the enrollment process must be completed. The objective of this enrollment process is to create a profile of the user. The process consists of the following two steps:

1. Sample Capture: the user allows for a minimum of two or three biometric readings, for example: placing a finger in a fingerprint reader. The quality of the samples, together with the number of samples taken, will influence the level of accuracy at the time of validation. Not all samples are stored; the technology analyzes and measures various data points unique to each individual. The number of measured data points varies in accordance to the type of device.
2. Conversion and Encryption: the individual's measurements and data points are converted to a mathematical algorithm and encrypted. These algorithms are extremely complex and cannot be reversed engineered to obtain the original image. The algorithm may then be stored as a user's template in a number of places including servers and ATM card.

A new and blank ATM card has to be enrolled with user details before it can be verified later. Enrollment system is usually operated by the admin to enter their customer details into the card. However, exception applies to the PIN entry where it should be entered by the user themselves and need to enter the PIN again to make sure they enter the correct ones.

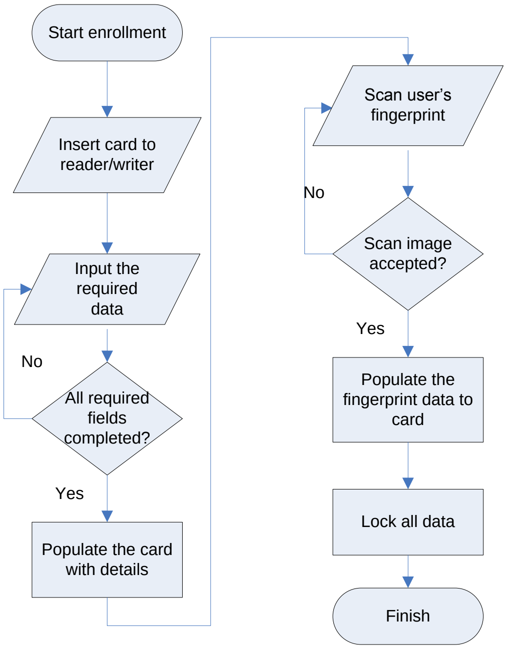
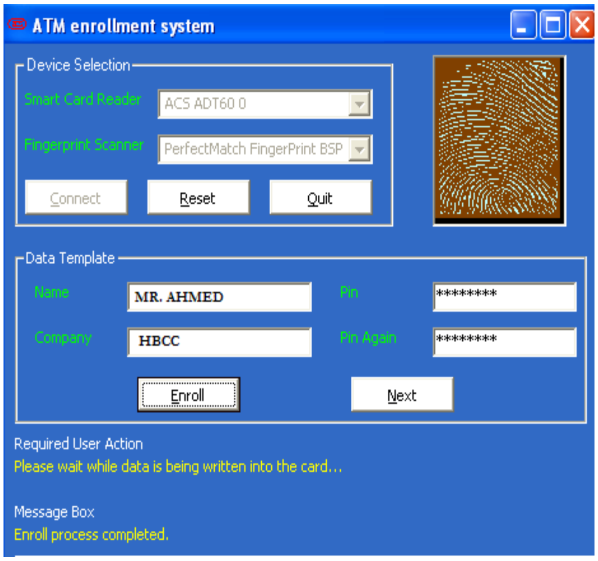

Start enrollment
Insert card to reader/writer
Input the required data
No
All required fields completed?
Yes
Populate the card with details
Scan user's fingerprint
No
Scan image accepted?
Yes
Populate the fingerprint data to card
Lock all data
Finish

Figure 1: Flowchart for the Enrollment Process



Smart Card Reader: ACS ADT60 0

Fingerprint Scanner: PerfectMatch FingerPrint BSP

Name: MR. AHMED

Company: HBCC

Pin: ********

Pin Again: ********

Required User Action

Please wait while data is being written into the card...

Message Box

Enroll process completed.

Figure 2: Enrollment Process

Identification and Verification - *Once* the individual has been enrolled in a system, he/she can start to use biometric technology to have access to his account via the ATM machine or related system to authorize transactions.

1. Identification: a one-to-many match. The user provides a biometric sample and the system looks at all user templates in the database. If there is a match, the user is granted access, otherwise, it is declined.
2. Verification: a one-to-one match requiring the user provides identification such as a PIN and valid ATM card in addition to the biometric sample. In other words, the user is establishing who he/she is and the system simply verifies if this is correct. The biometric sample with the

provided identification is compared to the previously stored information in the database. If there is a match, access is provided, otherwise, it is declined.

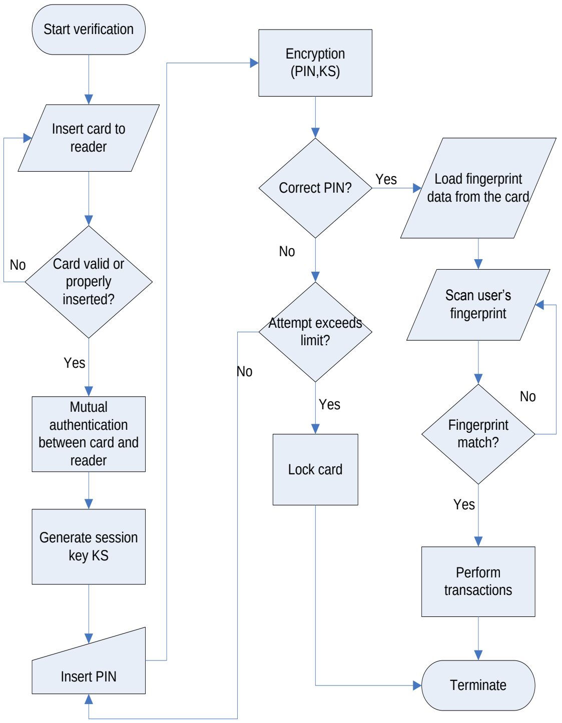
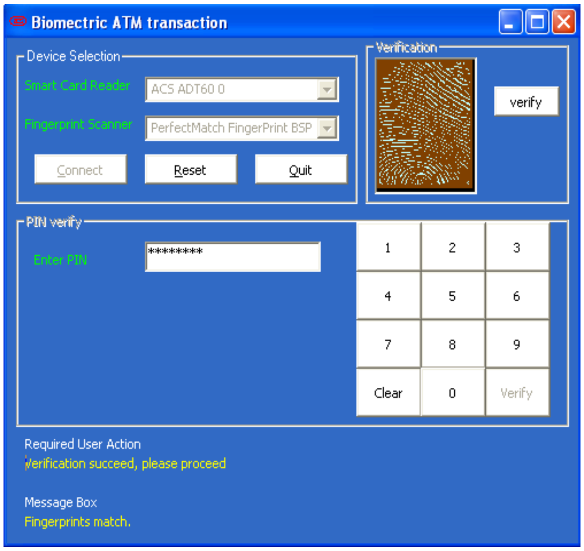


Figure 3: Flowchart for the Verification Process



Smart Card Reader: ACS ADT60 0

Fingerprint Scanner: PerfectMatch FingerPrint BSP

Enter PIN: *********

Required User Action

Verification succeed, please proceed

Message Box

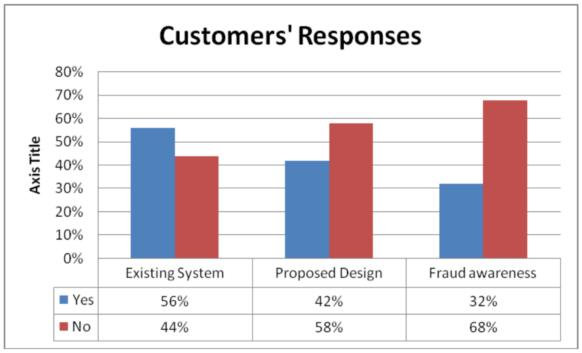
Fingerprints match.

Figure 4: Verification Process

After the card has been enrolled with user data, this particular card will be the user's ID. The PIN and fingerprint sample from the user were also encrypted and save into the card. In order to get access into the ATM machine, the user has to present the card to the card reader, and then verify the PIN and lastly matched their fingerprint detail with the card. In this particular system, the ATM interface is quite a simple one just showing the simple debit and credit function, what we tried to emphasis in our project is the complex verification part which includes the MAC and PIN encryption.

Customers' Perception

To understand the customer's perception, a simple research was conducted in Saudi Arabia. It is interesting that 56% of the users are convenient with the traditional ATM system while only 44% were not. Overall, a significant number of customers 68% were not aware about ATM frauds. When asked about the proposed design, 42% said they will be interested while 58% shows no interest. 63% said they would respond better if they knew much about ATM fraud and counter measures.



	Existing System	Proposed Design	Fraud awareness
🟦 Yes	56%	42%	32%
🟥 No	44%	58%	68%

Figure 5. Customers' Responses

IV. RISK ASSESSMENT

Despite the fact that more than half of the users involved in the survey are in favor of the traditional method (i.e. PIN and Card only), it is important for the banks to perform some risk analysis and decide whether to introduce the biometric scheme in the ATM system or not. In general, risks are assessed by evaluating preferences, estimating consequences of undesirable events, predicting the likelihood of such events, and weighing the merits of different courses of action. In this context, risk is formally defined as a set of ordered pairs of outcomes (O) and their associated likelihoods of occurrence.

Quantitative Risk Analysis Calculations

The key variables and equations used for conducting a quantitative risk analysis are shown below:

First, we need to determine the probability of loss caused by identified threat. This is known as the *exposure value* (EV). The value ranges from 0% to 100%.

Second, we need to determine a potential monetary loss factor for a single incident. This is known as the *single loss expectancy* (SLE).

Single Loss Expectancy (SLE) = Asset Value x Exposure Value. For instance, if the asset value is $1,000,000 and the probability of EV is 0.2, then;

SLE = 1,000,000 x 20% likelihood = $200,000

Third, we need to determine the annualized rate of occurrence (ARO). This is the estimated frequency a threat will occur within a year and is characterized on an annual basis. A threat occurring once in 10 years has an ARO of 0.1; a threat occurring 10 times in a year has an ARO of 10.

Finally, we need to determine how many times we could expect this loss to occur over a full year. This is known as the annualized loss expectancy (ALE). The formula to calculate ALE then is SLE x ARO. The summation of ALE can be defined as follows:

$$ALE = \sum_{k=1}^{n} \mathrm{I}(\mathrm{O}_k)\mathrm{F}_k$$

Where;
$\{O_1 \ldots\ldots O_n\}$ = Set of harmful outcomes
$I(O_k)$ = Impact of outcomes *k* in currency
F_k = Frequency of outcomes *k*

Assuming that based on the current system, ATM violations occur 10 times per year, then ALE is shown to be;

$200,000 x 10 = $2,000,000 ALE

The safeguard cost/benefit analysis or simply cost benefit analysis (CBA) = (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) = value of safeguard to the company.

Assuming that based on the proposed biometric ATM system, violations occur 1 times in 10 years; then ALE is shown to be;

$200,000 x 0.1 = $20,000 ALE

If the annual cost of the biometric security solution/safeguard is $10,000, then

CBA = $2,000,000 – ($20,000 +$10,000) = $1,970,000

Therefore, the bank stands to save, or avoid, over $2 million per year in potential losses by enforcing the biometric solution. Though, this does not mean that the bank will have $2 million as a profit line in the revenue report. However, it clearly makes sense to spend the $10,000 to avoid the potential $2 million annual loss.

CONCLUSION

Automatic Teller Machines have become a mature technology which provides financial services to an increasing segment of the population in many countries. Biometrics, and in particular fingerprint scanning, continues to gain acceptance as a reliable form of securing access through identification and verification processes. This paper identifies a high-level model for the modification of existing ATM systems to economically incorporate fingerprint scanning; and, outlines the advantages of using such system. It should be noted that the customers' perception cannot be generalized as it was highly affected by the tradition/culture of the users involves. It is a common practice in Saudi Arabia for some to assign his/her relative to perform ATM transactions such as bill payments, withdrawal and depositing on his/her behalf. In such case, biometric system will not be favored. As can also be seen from the statistic, there is lack of fraud awareness among the majority of the customers, it is therefore vital to ensure customers are aware about ATM fraud and preventive measures. Alternatively, the banks may also consider the biometric system as optional for those who are interested.

ACKNOWLEDGMENT

The author wishes to acknowledge Hafr Al-Batin Community College and King Fahd University of Petroleum and Minerals (KFUPM) Saudi Arabia for their support in providing the various facilities utilized in the presentation of this paper.

REFERENCES

[1]. NetWorld Alliance, "Timeline: The ATM's history", 2003, available online: http://www.atm24.com/NewsSection/Industry%20News/Timeline%20-%20The%20ATM%20History.aspx

[2]. "Global ATM Market and Forecasts to 2013", Retrieved May 7, 2010, from www.rbrlondon.com

[3]. ATM Market Place. (2009a). "ATM scam nets Melbourne thieves $ 500,000',” Retrieved December 2, 2009, from *http://www.atmmarketplace.com/article.php?id=10808*

[4]. ATM Market Place. (2009b). "Australian police suspect Romanian gang behind $ 1 million ATM scam'", Retrieved November 13, 2009, from *http://www.atmmarketplace.com/article.php?id=10883*

[5]. BBC News. (2009). "Shoppers are targeted in ATM scam'", Retrieved July 11, 2009, from *http://news.bbc.co.uk/2/hi/uk_news/england/tees/4796002*.stm

[6]. M. Bond. Understanding security APIs. Ph.D. Thesis, Computer Laboratory, University of Cambridge, 2004.

[7]. M. Bond and P. Zielinski, " Decimalisation table attacks for PIN Cracking",, Technical report (UCAM-CL-TR-560), Computer Laboratory, University of Cambridge, 2003.

[8]. M. Bond and P. Zielinski. Encrypted? Randomised? Compromised? (When cryptographically secured data is not secure).In Workshop on Cryptographic Algorithms and their Uses, Gold Coast, Australia, July 2004

[9]. O. Berkman and O. M. Ostrovsky. The unbearable lightness of PIN cracking. In Financial Cryptography and Data Security (FC), Scarborough, Trinidad and Tobago, Feb. 2007.

[10]. SpiderLabs. (2009). ATM Malware Analysis Briefing, Retrieved May 15, 2010, from https://www.trustwave.com/spiderLabs-papers.php

[11]. F. Deane, K. Barrelle, R. Henderson, & D. Mahar. "Perceived acceptability of biometric security systems". *Computers & Security*, Vol. 14, N. 3, pp. 225-231. 2005

[12]. B. Luca, S. Bistarelli, S. &A. Vaccarelli, "Biometrics authentication with smartcard", *IIT TR-08/2002*, Retrieved October, 9, 2009, from http://www.iat.cnr.it/attivita/progetti/parametribiomedici.html

Author profile and picture:

Lawan A. Mohammed receives his BSC (ED) degree in Mathematics and Education from ABU Zaria, Nigeria, MSc degree in Computer Science from DeMontfort University UK, and PhD degree in *Computer and Communication Systems Engineering* from University Putra Malaysia. Currently, he is an Assistant Professor at Hafr Batin Community College (KFUPM), Saudi Arabia. His research area is in the field secure network communication particular in the design of authentication protocol for both wired and wireless network.