International Journal of Computer Networks and Communications Security

VOL. 4, NO. 1, JANUARY 2016, 21–32
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Bring Your Own Device: Security Challenges and A theoretical Framework for Two-Factor Authentication

MORUFU OLALERE[1], MOHD TAUFIK ABDULLAH[2], RAMLAN MAHMOD[3] and AZIZOL ABDULLAH[4]

[1] Department of Cyber Security Science, Federal University of Technology Minna, Nigeria

[1, 2, 3, 4] Information Security Research Group, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Malaysia

E-mail: [1]lerejide@futminna.edu.ng, [2]taufik@upm.edu.my, [3]ramlan@upm.edu.my, [4]azizol@upm.edu.my

ABSTRACT

In this paper, the security challenges of BYOD are discussed, including existing security solutions which often are too restrictive. Data leakage is one of the security challenges confronting BYOD. Data leakage can occur as a result of stolen, lost or compromised employee devices. When an employee device is stolen, lost or comprised, an attacker can obtain access directly to the enterprise data on the employee device if a strong authentication technique is not in place. The traditional means of authenticating employees when connecting to an enterprise server in a traditional network environment which relies on either knowledge or ownership is too weak for the BYOD environment. In such a traditional enterprise network, employees obtain access to an enterprise server using their respective stationary desktop, while in a BYOD environment access to an enterprise server is from anywhere, making it easy for an attacker in possession of an employee device and password to gain unauthorised access. To address this problem, there is need for a strong authentication technique. This study proposes a theoretical framework for a two-factor authentication method that combines knowledge-based (Password) and biometric-based (Keystroke dynamic) features for authentication of mobile devices in a BYOD environment. Technical details on how the framework can be implemented are presented. It is the belief of the authors that proper implementation of the proposed potential future application framework will go a long way in addressing the problem of data leakage in a BYOD environment.

Keywords: *BYOD, Mobile Device, Authentication, Biometric, Keystroke Dynamic.*

1 INTRODUCTION

Using personal mobile devices for work has given rise to a trend called “bring your own device” or BYOD [1]. BYOD is defined as the use of devices owned by employees to access enterprise content and networks [2], [3]. The BYOD policy not only allows users to get access to enterprise data when at the work place, but also allows them to access the enterprise data from outside the enterprise environment. This trend brings many benefits for both employees and employers. When employees are empowered to choose the best device to get their work done, they become more mobile and productive. The business gains from having access to employees at anytime, anyplace, thus blurring the work-leisure divide, and in addition may actually further save costs by having the employee purchase the preferred device rather than providing it out of the corporate budget [4]. More benefits of BYOD can be found in [5]-[12].

However, as both the organisations and their employees are reaping the benefits of BYOD, so also they are concerned about the challenges of the BYOD policy [13]. One of the biggest challenges for organisations is that corporate data is being delivered to devices that are not managed by the corporate IT department, which has security implications for data leakage, data theft and regulatory compliance [11]. Ref. [14] points out that the real BYOD challenge is security and the real security challenge is not actually about the devices, it is about controlling access from the device to the corporate data. According to the literature, access control has been recognised as a key factor for addressing the security challenges of the BYOD policy.

While the security perimeter is being redefined, it is becoming increasingly apparent that passwords are no longer a sufficiently secure means of providing an identity in a BYOD environment [12]. In a traditional network environment, the enterprise does not allow outsiders (visitors) to work on the desktop of an employee. This makes it impossible for an attacker to gain unauthorised access to enterprise data through the employee desktop, even with knowledge of the employee login details. In fact, in most cases, the policies of many organisations do not allow visitors to employees to even sit close to an enterprise desktop.

However, in a BYOD environment, with the loss of an employee mobile device, or if the device is stolen, an attacker with knowledge of the employee login details can gain improper access to the enterprise data. Again, the policy of not allowing visitors to obtain access to an employee desktop in a traditional network environment is not practicable in a BYOD environment. The need for a new security parameter motivates the requirement for a two-factor authentication framework for mobile devices in a BYOD environment. This framework links the appropriate identity of an employee to a mobile device. In this present study, a two-factor combined knowledge (Password) and inherent action (Keystroke dynamic) are employed. It is important to note that this study only presents a theoretical framework for a two-factor authentication with details on how the framework works. Hence, experimentation is not presented in this study.

The rest of this paper begins with the BYOD security challenges and requirements. This is followed by existing methods of securing a BYOD environment. After this, various authentication techniques are discussed. Related work on authentication of mobile devices is also presented. The framework is then described with technical details of how each component of the framework functions. Finally, a conclusion is presented.

2 BYOD SECURITY CHALLENGES AND REQUIREMENTS

As both the employees and the enterprises are reaping the harvest of the BYOD policy, so also they are faced with the security challenges of that policy. A survey carried out by security vendor Trustwave found that ninety percent of vulnerabilities common in desktop computers were also present in mobile devices, regardless of the operating system [15]. Literature shows that data leakage, distributed denial of services, and malware are the most challenging security threats to BYOD [11].

2.1 Distributed Denial of Services

A Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. DDoS can deny regular employees the ability to run computer networked machines or their own personal devices. If there is no strong authentication mechanism, an attacker can pretend to be a legitimate user in order to carry out DDoS.

2.2 Malware

Malware is a malicious application that can affect both mobile devices and corporate applications. Mobile malware is an application with code embedded within it that compromises the security of the device or related data. When a device is compromised by malware, corporate confidential data can be lost and this can lead to background operation (sending text messages on behalf of the organisation that owns the data) by the attacker. Apart from devices compromised by malware, Corporate Applications can also be affected by a malware application, thereby making the application unusable or cause it to malfunction. A malicious application normally takes the form of a normal corporate application that has been injected with malicious code. Also a malicious application can be encountered when a user visits a compromised site. More details on how malware can affect BYOD can be found in [16].

2.3 Data leakage

Data leakage occurs as a result of access to enterprise data anywhere and anytime by employees. Data leakage means the availability of enterprise data in the hands of unauthorised users or recipients. The enterprise has little or no control over corporate data because corporate data is now accessed by using the personal device of an employee that has weak authentication methods.

Unauthorised access to the mobile device of an employee can cause data loss and data theft. Also, use of a too restrictive authentication method such as passwords etc. can cause data leakage. Leakage of data, such as company trade secrets, intellectual property or sensitive customer information such as credit card information can affect the reputation of an enterprise.

3 SECURING BYOD WITH MOBILE DEVICE MANAGEMENT (MDM) APPLICATIONS

MDM applications are developed to address some of the challenges of mobile devices (such as policy management, software distribution and Inventory management) that are not related to BYOD security challenges. More details on how MDM works can be found in [16]. Many enterprises see most of the MDM applications as a solution to the security challenges posed by BYOD.

However, MDM is not a complete solution to the BYOD security challenges. Ref. [17] predicts that by 2016, twenty percent of enterprise BYOD programmes will fail due to the deployment of mobile device management measures that are too restrictive.

4 USER AUTHENTICATION TECHNIQUES

In this section, different techniques of authentication are discussed for any platform, whether stand alone or a distributed system. Reasons are given why a particular authentication technique may not be suitable for the BYOD environment. Figure 1 shows the different categories of authentication techniques. These techniques with their weaknesses are discussed in the following sub-sections.

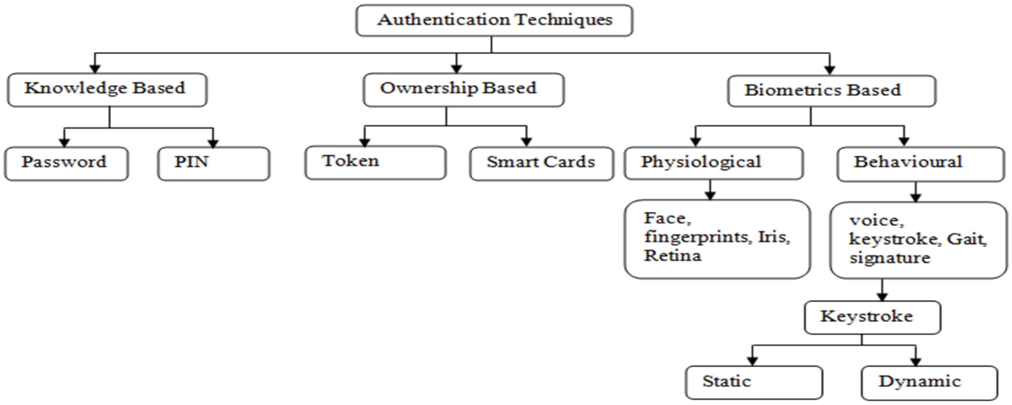

Fig. 1. Classification of User Authentication Techniques

4.1 Authentication based on Knowledge – "what you know"

Knowledge based authentication has to do with what a user knows [18]-[20] which is secret. Examples of knowledge based authentication are a Password which could be numerical, alphabetical or alphanumerical and a PIN which is a number that is commonly used by mobile devices. Implementation of a strong password and a security policy can prevent an unauthorised user or impostor from gaining access to a system. However, this technique suffers from vulnerability to shoulder surfing and brute force attack. If an attacker can obtain the user password through any of the above attack techniques, no matter how strong the password, the attacker will gain access to the system. Even without shoulder surfing or the brute force attack, if a system user gives the password away freely, no password policy, however strong, can prevent an unauthorised user from gaining access [19].

4.2 Authentication based on ownership/Object- "what you have"

Ownership based authentication relies on what a system user has [18], [21] which may be a token, smart card or a chip. This technique requires the system user to physically possess an object (such as a token or a chip) for authentication. The major problem with this kind of authentication arises when the system user loses the object to the attacker. If this object is in the hands of an attacker, unauthorised access can be gained into the system thus circumventing the authentication scheme. This implies that there is no assurance of uniquely identifying a legitimate user even with the ownership of an object [22]. Quite a number of systems today combine this technique with the knowledge based technique to improve the authentication scheme.

4.3 Authentication based on Biometrics/inherent- "what you are" and "what you do"

Biometric authentication relies on the physiological and behavioural characteristics of a system user [20]-[24]. References [23] and [25] defined biometric technologies as automated methods of verifying or recognising the identity of a living person based on physiological and behavioural characteristics. Biometric technology is an authentication mechanism that identifies users based on a unique characteristic. Ref. [26] mentioned the uniqueness of identity, non-transferability, impossibility to forget, difficulty in reproduction, usability with or without specific knowledge and complexity in alteration or modification as the benefits of biometric authentication compared to other authentication techniques. This unique characteristic could be based on what the user is (physiological), or what the user does (behavioural). Details of this two-fold biometric authentication technique are presented in the following sub-sections.

4.3.1 Physiological biometric- "what you are"

A physiological biometric simply means something that system users are. This type of biometric technology performs authentication based on the physical characteristics of a system user. Examples of physical characteristics used for authentication are fingerprints, the face, Retina pattern, and iris pattern. Physiological biometric authentication is reliable in the sense that the physical characteristics of a human being cannot be manipulated or duplicated. However, implementation of physiological biometric authentication requires additional hardware devices and software which often make the technique too expensive to implement. Also, some of the physiological authentication techniques require the collection of physiological features of a system user for training samples at different times under different conditions or moods. This creates inconvenience for the system users.

4.3.2 Behavioural biometric- "what you do"

A behavioural biometric simply means what the system user does. Behavioural biometric authentication relies on a behavioural characteristic of system users. Authentication is performed based on the pattern in which the system user does something. Examples of behavioural characteristics use for authentication are handwriting, handwriting signature, walking gait, voice, and keystroke dynamics. Behavioural characteristics are the unique characteristics of an individual that cannot be replicated. Some of these behavioural biometric authentication methods require hardware and software for their implementation while some require no hardware or software for their implementation. For instance, online (dynamic) signature verification uses a signature that is captured by pressure sensitive tablets that extract the dynamic properties of a signature in addition to the shape of the signature, while offline signature verification requires a scanner for scanning both the training and test samples. Keystroke dynamics is an example of behavioural biometric authentication that does not require additional hardware or software for its implementation. This makes it cheaper than any other biometric authentication technique.

4.3.2.1 Keystroke dynamics

Keystroke dynamics refers to the process of measuring, analysing and assessing the human typing rhythm on digital devices such as a personal computer keyboard, mobile phone keypad, smart phone touch screen [21], [22], [24], [27], [28]. Keystroke biometric authentication measures a typing pattern that is believed to be unique [29]. This type of behavioural biometric technique analyses the way a system user types on a digital device by monitoring the keyboard inputs thousands of times per second, and aims to identify users based on certain habitual typing rhythm patterns [23]. Keystroke dynamics authenticate a system user according to the pattern of typing. The principal concept behind keystroke dynamics is the ability of the system to recognise patterns, such as characteristic rhythms, during digital device interactions. Unlike physiological and some of the behavioural biometric authentication methods, keystroke dynamics does not require extra hardware or software (except the software for keystroke analysis) before implementation can take place.

In the keystroke dynamic authentication technique, there are two modes of authentication which are Static and Dynamic or continuous [21], [22]. The first refers to keystroke analysis performed only at specific times, for example during a login process, while the analysis of the typing rhythm is performed continuously during a whole session when the latter is applied, thus providing a tool to also detect user substitution after a successful login [23], [24]). The goal of continuous authentication is to ensure that the authorised identity is still whom they claim to be after the initial login procedure [22]. Substitution of a user after initial login by a legitimate user can be detected by dynamic authentication. Dynamic authentication mode involves continuous authentication throughout the system user operation, which means continuous typing must exist making it suitable for online examination authentication [19], [38] and making it unsuitable for the BYOD environment. Ideally, it is expected that only the secretary of any organisation will be involved in serious typing while other employees may not, making it difficult to propose dynamic authentication for the BYOD environment.

Unlike dynamic authentication, static authentication involves the use of keystroke dynamic biometrics with knowledge based authentication to come up with a login credential for a system user. Authentication in this mode is for login alone and substitution of the user after the initial login by a legitimate user cannot be detected by static authentication.

Considering the pervasive nature of the BYOD policy, the two-factor authentication method proposed in the present study is based on the static authentication mode of keystroke dynamics and a password. The following are the summarised properties that make keystroke dynamics suitable for mobile device authentication in a BYOD environment.

5 DESCRIPTION OF PROPOSED TWO-FACTOR AUTHENTICATION FRAMEWORK

The architecture of the proposed two-factor authentication technique is shown in Figure 2. The proposed framework consists of three main parts: the user interface, the enrolment phase and the authentication phase. The user interface serves as the platform in which both the enrolment and authentication processes begin. The enrolment and authentication of the employees' mobile devices takes place within the user interface. The details of the enrolment and authentication phases are given in the next section.

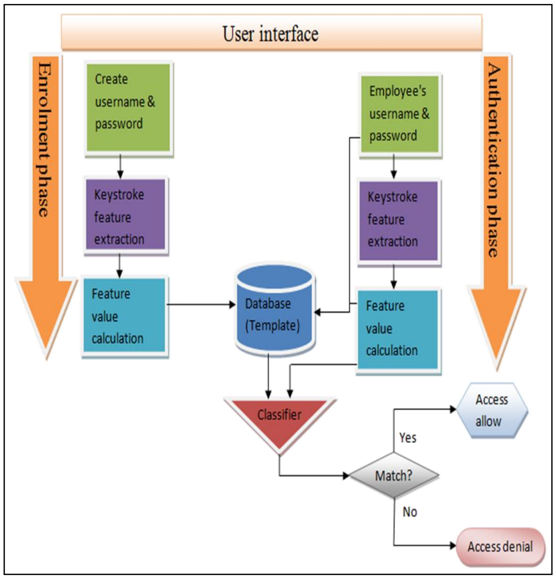
User interface
Enrolment phase
Create username & password
Keystroke feature extraction
Feature value calculation
Database (Template)
Employee's username & password
Keystroke feature extraction
Feature value calculation
Authentication phase
Classifier
Access allow
Yes
Match?
No
Access denial

Fig. 2. Architecture of two-factor authentication technique

5.1 *Enrolment phase*

The enrolment phase comprises of three stages: username and password creation (employee's profile registration), keystroke feature extraction and feature value calculation. The main purpose of the enrolment phase is to capture the typing pattern of an individual employee for template generation. The template is then stored in a database for future comparison/matching with the typing pattern of an employee seeking authentication.

5.1.1 *Employee's profile registration*

Generally, data acquisition is the first step in any biometric authentication technique. Data acquisition is the preliminary and essential stage of keystroke dynamics. This is performed via various input devices such as a normal computer keyboard, a customised pressure sensitive keyboard, a virtual keyboard, a special purpose number pad, a cellular phone or a smart phone [22]. In the proposed framework, data is acquired through the employee's profile registration. Each employee creates a username and a password during registration. The profile registration does not require any additional device other than the mobile device of employee. It is assumed that any mobile device will either have a keypad or a touchscreen for data input. The literature shows that keystroke dynamics have been experimented with on both the keypad and touchscreen of mobile devices. However, only a registered employee mobile device can be used to access the enterprise resources. Only the password will be trained for keystroke dynamic feature extraction as discussed in the next section.

5.1.2 *Keystroke feature extraction*

The next stage of the enrolment phase is feature extraction which is used to characterise the attributes common to all patterns belonging to a class [30]. The literature shows that keystroke dynamics are rich with distinctive feature information that can be employed for recognition purposes. Table 1 summarises different kinds of keystroke dynamic features commonly used by previous studies. However, the choice of keystroke dynamic feature(s) depends largely on many variables such as the environment in which the keystroke dynamics are applied and the device used to acquire the keystroke dynamic typing pattern.

Table 1: Commonly Used Keystroke Dynamic Features.

Keystroke feature	Description
Key hold time (Dwell time)	This is time interval between key presses until the key is released. This is also referred to as keystroke press time.
Digraph time (Flight time)	This is time interval between a key press and the next key press, a key release and the next key press, a key release and the next key release. That is, the time between a key release/press event of one key and a key press/release of another key. This is also referred to as keystroke latency.
Keystroke Pressure	This is a measure of the pressure applied to a key when pressed.
Typing speed	This measures the speed at which an individual types. Typing speed is the total number of keystrokes or words per minute.
Typing sound	Typing sound refers to the sound heard when a key is pressed.
Linguistic style	This has to do with language use as an individual difference.
Frequency of errors	This measures how often an individual makes a typing error. It is based on the use of the backspace key and the delete key.

For the purpose of the present framework, the keystroke press time and keystroke latency are considered. The following are the reasons for not considering the other keystroke features:

- Keystroke pressure and typing sound require pressure sensitivity and sound recording devices to be attached to a mobile device if not already available. This indeed contradicts the simplicity of the framework.
- Keystroke features such as typing rate, linguistic style and frequency of errors are only practical for text with many characters as input which is not applicable in the proposed framework as only characters for a password serve as input.

Figure 3 shows the keystroke dynamics feature extraction for the password "JIDE" with the following definitions:

"P" represents key press while "R" represents key release.

f_i^D represents the dwell time feature which is the time interval between the ith key press and the release of the same ith key. For $i = 1, 2, 3, \ldots K$, f_i^D is expressed as follows:

$$f_i^D = [f_1^D, f_2^D, f_3^D, \ldots, f_K^D] \qquad (1)$$

f_i^{L1} represents the keystroke latency (flight time) feature which is the time interval between the stroke of ith key press and the stroke of $(i+1)th$ key press. f_i^{L1} is expressed as:

$$f_i^{LI} = [f_1^{L1}, f_2^{L1}, f_3^{L1}, \ldots, f_{(K-1)}^{L1}] \qquad (2)$$

f_i^{L2} represents the keystroke latency feature which is the time interval between the stroke of the ith key release and the stroke of $(i+1)th$ key press. f_i^{L2} is expressed as:

$$f_i^{L2} = [f_1^{L2}, f_2^{L2}, f_3^{L2}, \ldots, f_{(K-1)}^{L2}] \qquad (3)$$

f_i^{L3} represents the keystroke latency feature which is the time interval between the stroke of the ith key release and the stroke of $(i+1)th$ key release. f_i^{L3} is expressed as:

$$f_i^{L3} = [f_1^{L3}, f_2^{L3}, f_3^{L3}, \ldots, f_{(K-1)}^{L3}] \qquad (4)$$

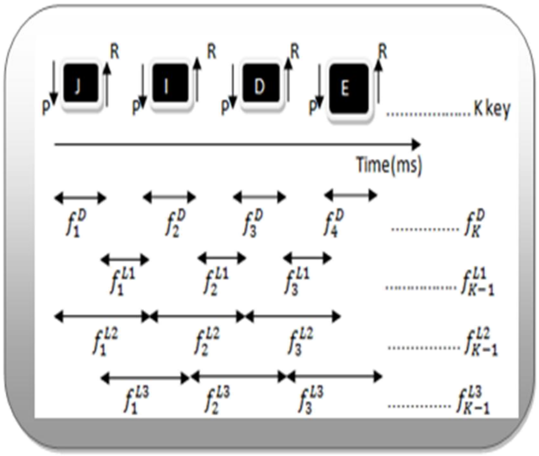

Fig. 3. Keystroke Dynamic Features Extraction for Password "JIDE"

5.1.3 *Feature value calculation*

The next stage in the enrolment phase is the feature value calculation. To generate the template of the typing pattern of a user, feature values must be calculated which represent the template of the user. Template generation is the stage where user's keystroke feature samples are combined and transformed into a compact yet representative form ([20]. To achieve this, the mean (μ) and standard deviation (σ) vectors for each feature $(i)$of f_i^D and $(f_i^{L1}, f_i^{L2}, f_i^{L3})$ are calculated using Equation (5) and Equation (6) respectively.

$$\text{Mean } (\mu_i) = \frac{1}{N}\sum_{j=1}^{N} f_{ij} \text{ ,} \qquad (5)$$

$$\text{SD } (\sigma_i) = \frac{1}{N-1}\sum_{j=1}^{N} \left| f_{ij} - \mu_i \right| \qquad (6)$$

where $j = 1, 2, \ldots, N. N$ represents the number of keystroke dynamics acquired for each user and

$f = f^D, f^{L1}, f^{L2}, f^{L3}$

The keystroke features, mean and standard deviation vectors of the user then serve as the keystroke dynamics template. These will be stored in the database for future authentication. Figure 4 represents the enrolment phase flow chart.

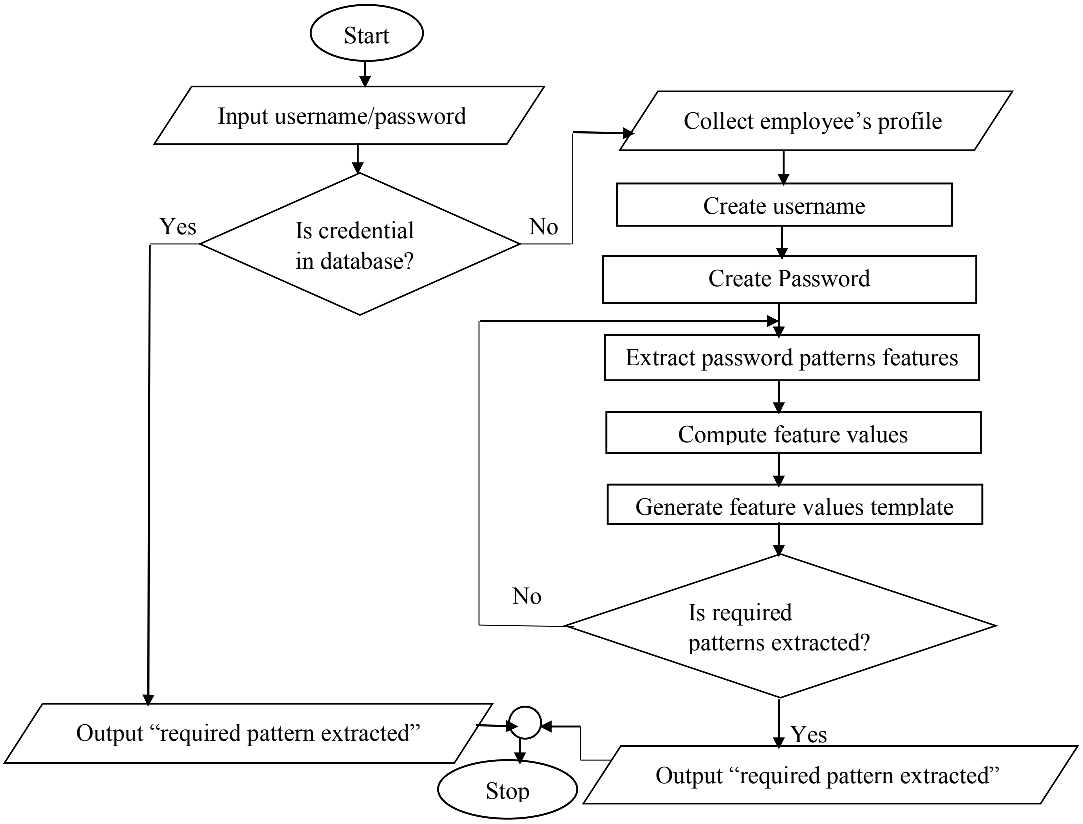
Start
Input username/password
Is credential in database?
Yes
No
Collect employee's profile
Create username
Create Password
Extract password patterns features
Compute feature values
Generate feature values template
Is required patterns extracted?
No
Yes
Output "required pattern extracted"
Output "required pattern extracted"
Stop

Fig. 3. Enrolment Phase Flow Chart

5.2 *Authentication phase*

During authentication, the employee makes an attempt to log-in by typing their username and password string. As the user types in the password, the keystroke dynamic features of the employee password are extracted as described in Section 5.1.2. The authentication phase uses a classifying method of authentication to either allow or deny the employee to log-in. The classifier verifies the similarity between the pattern of the password to be authenticated and the stored template of the prototype.

5.2.1 *Classifier*

For classification, a simple Euclidean distance classifier is proposed. A Euclidean distance measures the similarity between pattern vectors. In other words, the Euclidean distance computes the distance between the user reference template and the user seeking authentication. Assuming the reference feature vectors pattern is represented by Equation (7) and the test user feature vectors pattern is represented by Equation (8) given below:

$$R^F = \left[r_1^f, r_2^f, r_3^f, \dots, r_N^f\right] \qquad (7)$$

$$U^F = \left[u_1^f, u_2^f, u_3^f, \dots, u_N^f\right] \qquad (8)$$

Then, the Euclidean distance between the two N-dimensional vectors (7) and ((8) is expressed as:

$$D(R^F, U^F) = \left[\sum_{i=1}^{N} \left(r_i^f - u_i^f\right)^2\right]^{1/2} \qquad (9)$$

6 CHARACTERISTICS OF THE PROPOSED TWO-FACTOR AUTHENTICATION

The characteristics presented in Table 2 summarised why keystroke dynamic is considered for proposed two factor authentication techniques in BYOD environment.

Table 1: Characteristics of the proposed Two-Factor Authentication Technique for Mobile Devices in a BYOD Environment

Number	Characteristic	Description
1	Uniqueness	Keystroke dynamic characteristics are unique. This uniqueness is the result of the habitual typing rhythm patterns of an individual making it difficult to duplicate by an attacker or impostor. Even when an attacker gains access to the password of the legitimate user through password guessing or shoulder surfing or a brute force attack, the attacker cannot gain unauthorised access to the system (computer, mobile phone or database).
2	Low cost of production	Unlike Physiological biometrics and some of the behavioural biometric authentication methods that require additional hardware and/or software to implement them, keystroke dynamic authentication does not require additional hardware or software (except the software for analysis of the keystroke patterns) for its implementation.
3	Simplicity	Keystroke dynamics is very simple to construct and implement. The developer of keystroke dynamic analysis software does not need complex algorithms to extract typing patterns of the users and to come up with a classifier. Also, the users do not need to be overwhelmed with a different set of passwords, but rather need to create just a single strong password that will work with keystroke dynamics.
4	Convenience	Unlike physiological biometric authentication techniques, the keystroke dynamic authentication technique does not require a user to be subjected to the stress of feature extraction through the use of extra hardware such as a digital camera in the case of face recognition or a fingerprint machine in the case of fingerprint authentication. For instance, asking employees to face a digital camera under different conditions in order to capture their real feature template, which may cause an additional burden for the employees.
5	Easy to update	Generally, most behavioural biometrics change as time passes. Keystroke dynamic characteristics are not left out of this change. When changes occur, there is a need to update the database of the keystroke dynamic patterns of the employees by taking their typing patterns again. Amongst other behavioural biometric authentication techniques, keystroke dynamics are very easy to update.

7 RELATED WORK ON KEYSTROKE DYNAMIC AUTHENTICATION

Keystroke dynamics started gaining momentum as far back as the 20th century. Ref. [31] was the first researcher to suggest the use of keystroke characteristics for identification [32], [33]. In 1980, an investigation into whether keystroke dynamics could be used to identify an individual was carried out by [34]. According to the literature, their work is identified as the most primitive and significant research into the keystroke dynamic authentication technique [22], [27], [32], [35]. After the work of [43], keystroke dynamics become an active study area for researchers. Quite a number of researchers investigated the performance of the keystroke dynamic authentication technique in various domains where user authentication is needed. Some of these domains make use of keystroke dynamics and a knowledge based technique to create a strong authentication mechanism. These domains include a standalone desktop with a keyboard, mobile devices with keypads and Smart phones with a touch screen. Also included is the concept of the online examination with a desktop keyboard and cloud computing with mobile devices.

To investigate the performance of keystroke dynamics for desktop computer user authentication, [34] applied a statistical test on inter-key latencies to determine if the means of the keystroke interval time were the same. The study concluded that keystroke dynamics would be a good method for computer user authentication. The patent work of [36] used keystroke interval times as keystroke features to create a matching template vector using means and the covariance of keystroke interval times. The similarity of template vectors and verification vectors was used as the basis for classification. Another patent work of [37] extracted the time between keystrokes, the total time to type a predetermined number of characters and the pressure applied to various keys to form a keystroke feature template. Ref. [38] described a new approach to securing access to computer systems. The authors performed real-time measurements of the time durations between the keystrokes when a password was entered and by using pattern recognition algorithms, three on-line recognition systems were devised and tested with phrases and individual names as passwords. Ref. [23] used template matching and Bayesian likelihood models to address the practical importance of using keystroke dynamics as a biometric for authenticating access to workstations. Ref. [27] applied a vector based approach to identify keystroke patterns.

The keystroke dynamic feature extraction technique, the classifier technique, the mode of keystroke dynamics authentication, the effectiveness and platform on which the keystroke dynamic authentication technique can be applied are the main characteristics that differentiate the different research works concerning keystroke dynamics. A review by [30] summarised the well-known approaches (in terms of feature extraction and classification techniques) used in keystroke dynamics for mostly desktops and laptops. Also, [33] presented a representative subset of the research in keystroke dynamics at that time. Ref. [22] presented an up-to-date extensive survey that provided insightful details and a comparison of keystroke dynamic biometrics research performed throughout the previous three decades.

The rest of this review will focus on application of keystroke dynamics for mobile devices. Ref. [39] presented an investigation into the feasibility of using keystroke dynamics as a means of enhancing subscriber authentication on mobile handsets. Their feasibility study comprised of a number of investigations into the ability of neural networks to authenticate users successfully based upon their interactions with a mobile phone keypad. The results of their investigation produced 0 % false rejection and 1.3 % false acceptance. In a related work, [40] identified two typical handset interactions, entering telephone numbers and typing text messages, and sought to authenticate the user during their normal handset interaction. The study used neural network classifiers for classification and an average equal error rate of 12.8 % was achieved. Ref. [41] proposed a new approach for keystroke based authentication using a cellular phone keypad as an input device. The approach employed a statistical classifier and authenticated users using keystroke dynamics acquired when typing fixed alphabetic strings on a mobile phone keypad. According to the authors, the statistical classifier was able to perform user verification with an average equal error rate of about 13 %. A study by [42] reported the effectiveness of user authentication using keystroke dynamics-based authentication on mobile devices. The study found that a keystroke dynamic analysis system could be effective for mobile devices in terms of authentication accuracy.

In order to authenticate a legitimate user of a smart phone and to block imposters, [43] demonstrated that the keystroke dynamics of a smart phone user can be translated into a viable feature set for accurate user identification. They collected and analysed keystroke data of 25 diverse smart phone users and selected six distinguishing keystroke features that could be used for user identification. The authors showed that the six keystroke features for different users were diffused, so they therefore used a fuzzy classifier to cluster and classify the features. They finally provided a novel keystroke dynamics based PIN verification mode to ensure the security of smart phones with an average error rate of 2 % after detection mode and 0 % error rate of rejecting legitimate users. Ref. [24] discussed the feasibility of employing keystroke dynamics to perform user verification on mobile phones. They proposed a keystroke dynamics based verification method with application to the mobile phone and introduced a new statistical classifier for keystroke recognition. Their verification results indicated that the proposed approach could be effectively employed as a password hardening mechanism for cellular phones. The authors focused their attention on alphabetical passwords.

The project of [44] addressed weak authentication PIN codes on a smart phone by strengthening user authentication through keystroke dynamics. The study constructed and analysed four keystroke dynamic classifiers that made use of the sensors in a smart phone to learn the key tap behaviour of the true owner. The four classifiers tested were the Manhattan distance classifier, the Random forest classifier, the Gaussian discriminant analysis and a Support vector mechanism. It was reported that the support vector mechanism achieved remarkable results with a 5.6 % FAR (False Acceptance Rate) and a 7.6 % FRR (False Rejection Rate). Ref. [28] examined several time differences (for instance, a digraph) and checks for the suitability of keystroke authentication on touch screen keypads. Their study classified data from 152 subjects and with the additional features of the touchscreen, an error rate FRR of 4.59 % and a FAR of 4.19 % were achieved. Ref. [45] applied keystroke dynamic analysis with two novel keystroke features to support PIN based authentication for touch screen handheld mobile devices. The two novel keystroke features were pressure features and size features. Their result indicated that size features or pressure features could effectively promote the utility of a KDA (keystroke dynamics-based authentication) system in a PIN-based authentication schemes for touch screen handheld mobile devices.

However, it is important to note that all of the previous works for mobile devices consider native applications running on the device as the authentication entities except for the works of [26], [46]. Ref. [46] proposed a protocol for keystroke dynamic analysis which allowed web-based applications to make use of remote attestation and delegated keystroke analysis. Ref. [26] proposed a keystroke based authentication method for mobile cloud computing users. Different from the two studies presented above, this present study proposes a two-factor authentication technique which is based on password and keystroke dynamics which will allow an enterprise to remotely authenticate an employee's mobile device seeking access to the data of the enterprise.

8 CONCLUSION

There is no gainsaying in the fact that BYOD has come to stay in both the developed economies and the emerging economies of the world. It is also known that the BYOD policy has not only come with benefits but also with challenges. The authors of the present study have discussed the benefits and challenges of the BYOD policy. However, security challenges top the list of the difficulties confronting the BYOD policy. Data leakage is one of the security challenges. In order to address this security challenge, this study proposes a two-factor authentication technique for mobile devices in a BYOD environment. It is the hope of the authors that this proposition will go a long way in assisting the captains of industry and enterprise information technology departments to solve the problem of mobile device authentication in their enterprises.

9 REFERENCES

[1] Gheorghe, G., and Neuhaus, S., "Poster: Preserving privacy and accountability for personal devices", CCS' 13, 4 Nov. – 8 Nov., 2013. Berlin, Germany: pp. 1359 – 1361.

[2] Deloitte, Understanding the bring-your-own-device landscape. A Deloitte research report, 2013. Retrieved March 20, 2014 from http://www.deloitte.com/assets/Dcom-Guam/Local%20Assets/Documents/Technology,%20Media%20and%20Telecommunications/Understanding%20the%20bring-your-own-device%20landscape.pdf.

[3] Li, F., Peng, W., Huang, C. and Zou, X., "Smart phone strategic sampling in defending enterprise network security", IEEE International Conference on communication. 9-13 June, 2013 Budapest: pp. 2155 – 2159.

[4] Mahesh, S., & Hooter, A., Managing and securing business networks in the smartphone era (Management Faculty Publications, Paper 5). 2013. Retrieved from http://scholarworks.uno.edu/mgmt_facpubs/5

[5] Citrix®, Best practices to make BYOD simple and secure. White paper, 2013. Retrieved

March 8, 2014 from http://www.citrix.com/content/dam/citrix/en_us/documents/oth/byod-best-practices.pdf.

[6] EY, Bring your own device: Security and risk considerations for your mobile device program. Insights on governance, risk and compliance, 2013 Retrieved March 20, 2014, from http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf.

[7] Kerravala, Z., Bring-your-own-device requires new network strategies. ZK Research, 2012. Retrieved Febuary 10, 2014, from http://www.xirrus.com/cdn/pdf/zeusk_byod_requires_new_network_strategies.

[8] Hayes, J., "The device divided", Engineering and Technology, vol. 7, No. 9, 2012, pp. 76 – 78.

[9] Disterer, G. and Kleiner, C., "BYOD Bring your own device", Procedia Technology 9, 2013, pp. 43-53.

[10] Miller, K. W., Voas, J. and Hurlburt, G. F., "BYOD: Security and privacy considerations", IT Professional, vol. 14, No. 5, 2012, pp. 53-55.

[11] Morrow, B., "BYOD security challenges: control and protect your most sensitive data", Network Security, (2012)12, pp. 5-8.

[12] Edwards, C., "Identity- the new security perimeter", Computer Fraud & Security, (2013)9, pp. 18–19.

[13] Olalere, M., Abdullah, M. T., Mahmod, R., and Abdullah, A., "A review of bring your own device on security issues", SAGE Open, vol. 5, no. 2, 2015, pp. 1-11

[14] Thielens, J., "Why API are central to a BYOD security strategy", Network Security, (2013) 8, pp. 5-6.

[15] Leavitt, N., "Today's mobile security requires a new approach. IEEE Computer Society, Vol. 46, No. 1, 2013, pp. 16- 19.

[16] MTI Technology, Bring your own device. The future of corporate computing. MTI white paper, 2014. Retrieved September 20, 2014, from https://mti.com/Portals/0/Documents/White%20Paper/MTI_BYOD_WP_UK.pdf.

[17] Gartner, Gartner Says Less Than 0.01 Percent of Consumer Mobile Apps Will Be Considered a Financial Success by Their Developers Through 2018. Gartner Newsroom, 2014. Retrieved April 22, 2014, from http://www.gartner.com/newsroom/id/2648515

[18] Shepherd, S. J., "Continuous authentication by analysis of keyboard typing characteristics", European Convention on Security and Detection. 16 May-18 May, 1995. Brighton, UK, pp.111-114.

[19] Flior, E., and Kowalski, K., "Continuous biometric user authentication in online examination", Seventh International Conference on Information Technology. IEEE Computer Society. 12-14 April, 2010, Las Vegas, pp. 488-492.

[20] Ramu, T. and Arivoli T., "A framework of secure biometric based online exam authentication: an alternative to traditional exam", International Journal of Scientific and Engineering Research, Vol.4, No. 11, 2013, pp. 52-60.

[21] Shanmugapriya, D., and Padmavathi, G., "A survey of biometric keystroke dynamics: approaches, security and challenges", International Journal of computer Science and Information Security, Vol. 5, No. 1, 2009, pp. 115-119.

[22] Teh, P. S., Teoh, A. B. J., and Yue, S., "A survey of keystroke dynamics biometrics", The Scientific World Journal, 2013, pp. 1-24.

[23] Monrose, F., and Rubin, A. D., "Keystroke dynamics as a biometric for authentication, Future Generation Computer Systems. (16)2000, pp. 351–359.

[24] Maiorana, E., Campisi, P., Gonzalez-Carballo, N., and Neri, A., "Keystroke dynamics authentication for mobile phone", Proceedings of the 2011 ACM Symposium on Applied Computing, 21-25 march, 2011 Taichung, Taiwan, pp. 21-26.

[25] Jain, A. K., Ross, A., and Prabhakar, S., "An Introduction to Biometric Recognition," IEEE Trans. Circuits and Systems for Video Technology, vol. 14, no. 1, 2004, pp. 4-20.

[26] Babaeizadeh, M., Bakhtiari, M., and Maarof, M. A., "Keystroke dynamic authentication in mobile cloud computing", International Journal of Computer Application, Vol. 90, No 1, 2014, pp. 29-36.

[27] Guven, A., and Sogukpinar, I., "Understanding users' keystroke patterns for computer access security", Computer and Security. Vol. 22, No. 8, 2003, pp. 695-706.

[28] Trojahn, M., Arndt, F., and Ortmeier, F., "Authentication with keystroke dynamics on Touchscreen kaypads-effect of different n-graph combinations", MOBILITY 2013: The Third International Conference on Mobile Services, Resources, and User. 17 – 22 November, 2013, Lisbon, Portugal, pp. 114-119.

[29] Stewart, J. C., Monaco, J. V., Cha, S.-H., and Tappert, C. C., “An investigation of keystroke and stylometry traits for authenticating online test takers”, Proceeding of the International Joint Conference on Biometrics (IJCB `11). Washington, DC. 11-13 October, 2011, pp. 1-7.

[30] Karnan, M., Akila, M., and Krishnaraj, N., “Biometric personal authentication using keystroke dynamic: a review”, Applied Soft Computing, Vol. 11, No. 2, 2010, pp. 1565-1573.

[31] Spillane, R., “Keyboard apparatus for personal identification”, Technical report. IBM Technical Disclosure Bulletin, Vol. 17, No. 11, 1975, pp. 3346-3346.

[32] Peacock, A., Ke, X., and Wilkerson, M., “Typing patterns: A key to user identification”, IEEE on Security and Privacy, Vol. 2, No. 5, 2004, pp. 40-47.

[33] Crawford, H., “Keystroke dynamics: characteristics and opportunities”, Eighth Annual International Conference on Privacy, Security and Trust. 17-19 August 2010, Ottawa, pp. 205-212.

[34] Gaines, R., Lisowski, W., Press, S., and Shapiro, N., “Authentication by keystroke timing: some preliminary results”, Technical Report Rand Rep. R-2560-NSF, RAND Corporation, 1980.

[35] Teh, P. S., Teoh, A. B. J., Tee, C., and Ong, T. S., “Keystroke dynamics in password authentication enhancement”, Expert System with Applications, Vol. 37, No. 12, 2010 pp. 8618-8627.

[36] Garcia, J., “Personal identification apparatus”, U.S. Patent Number 4,621,334, November 4, 1986. Retrieved November 3, 2014, from http://www.google.com/patents/US4621334.

[37] Young, J. R., and Hammond, R. W., “Method and apparatus for verifying an individual’s identity”, U.S. Patent Number 4,805,222, 1989. Retrieved November 5, 2014, from http://www.google.com/patents/US4805222A.

[38] Bleha, S., Silvinsky, C., and Hussien, B., “Computer-access security systems using keystroke dynamics”, IEEE Transactions on Pattern Analysis and Machine Intelligence, vVol. 12, No. 12, 1990, pp. 1217–1222.

[39] Clarke, N. L., Furnell, S. M., and Reynolds, P. L., “Subscriber authentication for mobile phone using keystroke dynamics”, Proceedings of the Third International Network Conference (INC 2002). Plymouth, UK, pp. 347-455

[40] Clarke, N. L., and Furnell, S. M., “Advance User authentication for mobile devices”, Computer and Security, Vol. 26, No. 2, 2007, pp. 109-119.

[41] Campisi, P., Maiorana, E., Bosco, M. L., and Neri, A., “User authentication using keystroke dynamics for cellular phones”, IET Signal Process, Vol. 3, NO. 4, 2009, pp. 333-341.

[42] Hwang, S., Cho, S.-s., and Park, S., “Keystroke dynamics-based authentication for mobile devices. ScienceDirect Computer and Security, Vol. 28, No. 1-2, 2009, pp. 85-93.

[43] Zahid, S., Shahzad, M., Khayam, S. A., and Farooq, M., “Keystroke-based user identification on smart phones”, Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection (RAID). Semptember, 2009, Berlin, Heidelberg, pp. 224-243.

[44] Ho, G., “Tapdynamics: strengthening user authentication on mobile phones with keystroke dynamics”, Technical report, Stanford University, 2014.

[45] Tasia, CJ., Chang, TY., Cheng, PC., Lin, JH. “Two novel biometric feature in keystroke dynamics authentication system for touch screen devices”, Security Comm. Networks 2014(7), pp. 750-758.

[46] Nauman, M., and Ali, T., “Token: trustable keystroke-based authentication for web-based applications on smartphones”, Information Security and Assurance. (76)2010, pp. 286-297.