Performance and Security Evaluation of Biometric-Based Web Application

Okafor, Friday Onyema and Ogbuabor, Godwin

Department Of Computer Science,
Michael Okpara University of Agriculture, Umudike
E_Mail: Okafor.Friday@Mouau.Edu.Ng, Goddyogbuabor@Yahoo.Com

Abstract

Biometric recognition is the use of individual biometric physical or behavioural characteristics such as iris, retina, and fingerprint to uniquely identify the person. This technology offers a reliable and convenient solution to the problem of personal recognition. Fingerprint identification and verification system is the most widely used today due to ease of implementation and high performance. With the increase in the use of biometric systems in various sectors and organisations, there is increasing concern about the security and privacy of persons involved. Deploying a biometric system on the web makes it accessible by everybody thus preventing hackers and imposters that might exploit the system for their own gain. This paper evaluates the performance and security of biometric based web application, narrating the importance and challenges of using biometric to identify individuals in the web. To evaluate the system, Student Attendance Monitoring System was developed using java technology and MYSQL as the backend. The system involves scanning of student fingerprint using fingerprint scanner. Fifty (50) students were enrolled into the system and success rate of above 93% was recorded. The template is also secured due to the encrypted nature of the extracted template of the students fingerprint during enrolment and identification processes.

Keywords: Web Application, Security, Performance, Biometrics

Introduction

The increase in web application deployment has created complex tools that are problematic to secure in our society today. Most organisations depend on the security measures at the perimeter of network, example firewalls, in order to secure their information technology infrastructure; traditional network security may not be enough to safeguard web applications from such threats.

Banks and financial institutions have flooded customers mail box with emails, stressing the need to avoid disclosing customers' login details to third party irrespective of the person that demand for it. This is due to the unreliable nature of the use of password and username.

Due to the increase in the web application attacks; highly reliable and convenient personal verification and identification technologies are vital in our society today [25].

Web applications are accessed through browsers and can be accessed by any one provided that the person has internet connectivity. This shows the possibility of both good and bad intended users to gain access to the application through the browser.

Teodoro and Serrao [23] stated that the National Institute of Standards and Technology (NIST) held a National Vulnerability Database (NVD), which has over 4000 vulnerabilities identified in the application level as of March 2010. They highlighted that it was confirmed by the Gardner Group, which estimated that 70% of attacks to company's web application come from the application level. With this, it is obvious that we need to secure our application from the application level and not depending only on the network and host security.

Numerous researches and workshops have been conducted to look into web application vulnerabilities that have put different business organisations, Education sectors and industries into sleepless night. Major organisations and government departments have devoted resources to develop strategies, policies and guidelines aimed at managing the risks from the open nature of web applications.

But despite all this measures, hackers and attacker still penetrate into organisation records through the open nature of web application leading to violation of people's information rights.

The problems faced in difference organizations today is not only limited to authenticating users through the browser, because if access is gained to the database through the host, the imposter can get the authentication details and use it to carry out illegal transactions.

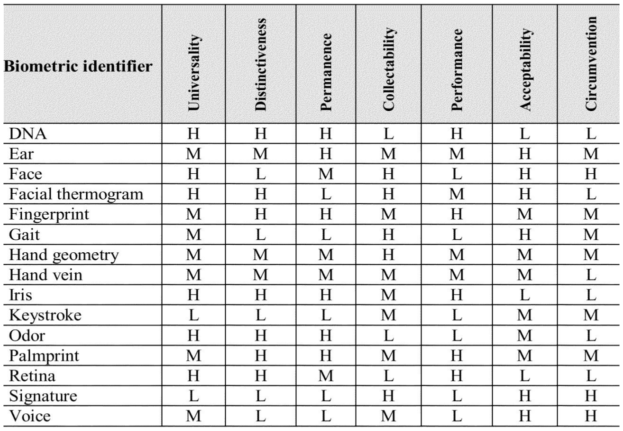
Most login details are encrypted but this is not sufficient to safeguard the information as the encrypted username and password can be decrypted and be used to gain access to the application illegally.

Biometrics, which uses the distinctive physiological and behavioural characteristics to recognize the identity of an individual has been proven to show high level of security since it is impossible to have two individuals with the same biometric features. There are different biometric tools that can be used to verify and identify individuals based on their physiological characteristics, as for instance the use of Iris, Face recognition, Retina and Fingerprint. Most of these have been proven to be almost 100% accurate and reliable.

Fingerprint biometrics is gaining geometric popularity in governmental, educational, military, and commercial security applications these days. Therefore, to evaluate the performance and security of web application using fingerprint biometrics, the **Student Attendance Monitoring System** was developed. Fingerprint biometric was chosen for this project because of its level of accuracy and global acceptability.

The application '**Student Attendance Monitoring System' is** developed using Java Technology and Relational Database Management System (RDMS) to monitor attendance of students to lectures.

According to different authors and researchers, using fingerprint biometrics to authenticate users has shown high level of performance. But the question is: has it solved the problem of security in the internet world? This will be determined by the end of this work-after evaluation of the web application (Student Attendance Monitoring System).



Biometric identifier	**Universality**	**Distinctiveness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Circumvention**
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Figure 1: Comparison of various biometric technologies based on the perception of the authors.

High, Medium, and Low are denoted by H, M, and L, respectively (Jain *et al,* 2004*)*.

Related Works

The use of fingerprint biometric system is not a new technology in the society; the technology has been applied by different enterprises and organisation to verify or identify individuals based on their physiological characteristics. Lots of researches have been conducted on fingerprint recognition system by different authors and researchers, both in the educational sectors and in the industries. New discoveries are made almost every day on the quest to maximize the accuracy, performance and security of different systems using fingerprint biometric system. The history of fingerprint as a means of identifying individuals was initiated by the Babylonians. The ancient Babylonian conducted business transaction by pressing the tips of their fingertips into clay [24]. The use of fingerprint as a valid means of identification was formally accepted by the law-enforcement agencies in the early 20th century [13]. For the fact that this is not the first work on fingerprint biometric system, it is therefore very important to review related works.

Saraswat and Kumar [21], in their work, were more concerned about the accuracy and efficiency of fingerprint verification system. They pointed out that manual means of attendance is a laborious and troublesome work and wastes a lot of time. The aforementioned problem led to their development of new system using fingerprint verification techniques. Saraswat and Kumar [21] were convinced from their experimental result that using fingerprint as a means of verification is highly efficient. In their work, they highlighted that fingerprint verification and authentication is most popular means to identify and verify individuals where security is put into consideration. They also stated that the use of fingerprint as a means of verification of individuals is highly convenient and reliable.

This is in accordance with what Shoewu and Idowu [22] pointed out in their work that Automated Attendance Management System using biometrics would provide solution to the errors and waste of time nature of the manual system.

Shoewu and Idowu [22] used eighty candidates to evaluate their system (Attendance Management System Using Biometrics) and success rate of 94% was recorded. The 6% failure rate might be due to incorrect position of students' finger during enrolment. From the experiment conducted by the authors, the average execution time of the manual attendance system for the eighty students were 17.83 seconds while for the automated management system using biometrics was 3.79 seconds. Also from their experiment, they argued that automated system using biometrics shows higher performance over manual system. Finally, they recommended that the system should be modified into web based system. This created an avenue for the system to be accessed anywhere in the school provided that there is internet connectivity and reduce the cost of networking systems (computers) or accessing the application in only one classroom.

Mohammed and Kameswari [17] implemented the web based student attendance system as recommended by Shoewu and Idowu [22], but they used RIFID (Radio Frequency Identification) Technology. Radio Frequency Identification is the use of wireless non-contact radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. They stated that this will enable lecturer access the system over the web and report can be generated anywhere, provided there is internet connection. Mishra et al [16] argued that using RFID creates the problem of students carrying cards and also RFID detectors have to be installed, thereby, creating extra expenses. Furthermore, implementing the attendance system to be accessed over the internet creates security risk, as this can be accessed by hackers and imposters.

Kawaguchi et al [11] worked on attendance system using face recognition technology. This technology identifies individuals by extracting his/her facial physical features and compares it with the template stored in the database. They pointed out that face recognition rate is not sufficiently high, which is in accordance with the **figure 1** above by

Jain et al [6]**.** To increase the performance rate of the system, they implemented a system that estimates the attendance as well as the position of each student by continuous observation and recording. They were convinced from their experiment that continuous observation improves the performance rate of the face recognition system. But this entails that students must maintain their position in class during each lecture.

Attendance Monitoring System using iris recognition system was also carried out by Kadry and Smaili [10]. They argued that personal authentication system based on iris recognition is the most reliable among all biometrics methods. This confirmed what Hsiung and Mohamed 5] stated that "Iris recognition system is the most reliable system for an individual identification". They pointed out that the probability of finding two people with identical iris pattern is almost zero. They also argued that iris recognition system is more stable compared to fingerprint biometrics system. *"*Iris is protected from the external environment behind the cornea and the eyelid. It is not subject to deleterious effects of aging, the small-scale radial features of the iris remain stable and fixed from about one year of age throughout life"[10]. Despite the advantages over other biometrics methods, Iris recognition system is very expensive and it requires much memory for data storage [12].

Fingerprint biometric technology can also be implemented in payment system. Kumar and Ryu (2008), in their paper stated that *Biometric* payment system is reliable, economical and it has more advantages as compared with others means of payment such as credit and debit card.

In fact, this method will greatly improve payment system. Instead of remembering password and username, the customers will just scan his/her fingerprint and if authenticated, the payment will be made. They stated that this system is used by some companies such as **SHELL in Chicago, USA** to accept payment from their customers. This system will also ensure that the owner of the account is the person making the payment by himself. Cards such as VISA card has everything that customer need to make payment or write on it, if stolen by bad person, the person can use the card to carry out transaction successfully. Using biometric system will eliminate this risk since the individual has unique biometric features that can be used to identify the person which no other person has.

The importance of fingerprint biometric system cannot be overemphasised because it has been proved as one of the best means of identifying individuals, unlike password and PIN(Personal Identification Number) means of identification, this technology ensures the person involved is present.

From the works done so far by different authors and researchers, using fingerprint as a means of identification and verification in taking students attendance is a welcome idea as this prevents impersonation, thereby forcing students to always be in the class during exam, lecture and laboratory work.

Moreover, from the researches done so far by different authors and researchers, the emphasis has been on the efficiency, accuracy and performance of Attendance Monitoring System using biometrics, neglecting the fact that peoples' data need to be properly secured.

This work will go beyond the performance of the system to evaluating the security of web application (Student Attendance Monitoring System) using fingerprint biometric.

Fingerprint Biometric System

Biometric is regarded as the automated technique of measuring a physical characteristic of a person for the purpose of recognizing him/her [4]. They include fingerprint, face, retina, iris, etc.

Biometric system is a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database [8]. Biometric system is not a new technology since this has been applied in different facet of life for different purposes, such as medical system, library system, attendance system etc.

Some people adopt biometric technology because of its high level of performance while some consider it as a means of ensuring high security [20].

Biometric system operates in two different modes:

1. Verification Mode
2. Authentication Mode

Verification Mode

In this mode, the system validates the person's identity by comparing the captured biometric data with the stored biometric template.

Identification Mode

In this mode, individuals are recognized by searching through the templates stored in the database.

Fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of child's development [8]. Even fingerprint of identical twin are different which makes reliance on fingerprint authentication reliable. Humans have used fingerprints for personal recognition for many years and the matching accuracy using fingerprints has been shown to be very high [8].

How Fingerprint Biometric works

A fingerprint of an individual consists of series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint is determined by the pattern of ridges and furrows as well as the minutiae points. These points are local ridge characteristics that occur when a ridge splits apart or a ridge ends [2].

During enrolment process, the fingerprint scanner sensor scans the user's fingerprint which is then converted to digital image. The minutiae extractor processes the fingerprint image to identify specific details known as minutia points that are used to distinguish different users [7].

A good-quality fingerprint image contains about 20-70 minutiae points; the actual number depends on the size of the sensor surface and how the user places his finger on the sensor during enrolment. The system stores the minutiae information - location and direction along with user's information as a template in the database [6][7][8][9].

During identification process, "the user touches the same sensor, generating a new fingerprint image called a *query print*. Minutia points are extracted from the query print, and the matcher module compares the query minutia set with the stored minutia templates in the enrolment database to find the number of common minutia points. Due to variations in finger placement and pressure applied on the sensor, the minutia points extracted from the template and query fingerprints must be aligned, or registered, before matching. After aligning the fingerprints, the matcher determines the number of pairs of matching minutiae—two minutia points that have similar location and directions. The system determines the user's identity by comparing the match score to a threshold set by the administrator" [6][7][8][9].

The identification and matching process takes less than one second to complete [2]. This depends on the environment where the system is hosted as there are many factors that delay the execution of the program such as bridge in network transmission. The figure below shows the process involved in the extraction of the fingerprint template.

There are two types of recognition errors in fingerprint biometrics: False accept rate and false reject rate. Fingerprint identification system performance is measured in terms of its false accept rate (FAR) and false reject rate (FRR). If a non-matching pair of fingerprints is accepted as a match, it is called a false accept while if a matching pair of fingerprints is rejected by the system, it is called a false reject [19][20].

Ethical Issues in the use of Biometric Technology

The use of fingerprint biometric to identify and verify individual is quite enamours. It has been applied in different organisations for better performance and security purposes. However, there are serious ethical issues in the use of biometric technology [1].

In spite of the performance and security benefits offered by fingerprint biometrics system, issues concerning the individual beliefs, personal privacy, and protection arise as a result of the use of biometric which involves extracting physiological or behavioural characteristics of individuals that is unique to the person. Some Religious objections interpret biometrics recognition as "the mark of beast" by citing somewhat dubious biblical references [6]. Some users have also raised concerns about the hygiene of biometric scanners that requires contact with the human body. Given that we routinely touch many objects such as money that are also touched by strangers, this objection may be considered frivolous excuses [6].

Moreover, as a result of difference threats around the globe such as security, illegal immigration identity theft and fraud etc. it is now important to implement biometric system for better identification and verification. "The public concern regarding the issues mentioned above cannot be ignored. There is a compelling need to find "Workable and Deployable" solutions to these issues" [1].

Fingerprint Biometric Security Threats

The features extracted from the fingerprint digital image are sensitive information of individuals that is unique to the person. If the template is stolen, it is stolen forever since it has no duplicate. This has raised security issues about the use of biometric for identification and verification of individuals. Applications available on the web can be accessed by anybody that has internet connectivity; both good and bad personalities have access to the system. Since this is available online, there are serious security threats. Hackers and attackers can gain access to the database and compromise fingerprint templates.

Attacks

Ratha et al [20] identified eight possible attacks in biometrics system. These possible attacks are discussed below

1. Presenting fake biometrics at the sensor: reproduction of the biometric feature is presented as input to the system in this mode of attack e.g. fake finger.
2. Resubmitting previously stored digitized biometrics signals: In this mode of attack, a recorded signal is replayed to the system, bypassing the sensor e.g. the presentation of an old copy of a Fingerprint image.
3. Overriding the feature extraction process: in this mode, the feature extractor is attacked using a Trojan horse, so that it produces feature sets preselected by the intruder.
4. Tampering with the biometric feature representation: The features extracted from the input signal are replaced with a different, fraudulent feature set (assuming the representation method is known). Often the two stages of feature extraction and matcher are inseparable and this mode of attack is extremely difficult. However, if minutiae are transmitted to a remote matcher (say, over the Internet) this threat is very real.
5. Corrupting the matcher: The matcher is attacked and corrupted so that it produces preselected match scores.
6. Tampering with stored templates: The database of stored templates could be either local or remote. The data might be distributed over several servers. Here the attacker could try to modify one or more templates in the database, which could result either in authorizing a fraudulent individual or denying service to the persons associated with the corrupted template. A smartcard-based authentication system, where the template is stored in the smartcard and presented to the authentication system, is particularly vulnerable to this type of attack.
7. Attacking the channel between the stored templates and the matcher: The stored templates are sent to the matcher through a communication channel. The data travelling through this channel could be intercepted and modified.
8. Overriding the final decision: If the final match decision can be overridden by the hacker, then the authentication system has been disabled. Even if the actual pattern recognition framework has excellent performance characteristics, it has been rendered useless by the simple exercise of overriding the match result.

Countermeasures

Ratha et al [20] also presented the following countermeasures to prevent the possible attacks identified in biometric system.

1. Finger conductivity or fingerprint pulse at the sensor can prevent attackers from presenting fake biometrics at the sensor.
2. Encrypted communication channels will go a long way in eliminating attack on the biometric features.
3. Encrypting the extracted template will prevent using the template to gain access except if the hacker has the encryption key.

Template Protection

The growing use of biometric has given concern on the privacy and security of the stored biometric data. Due to the uniqueness of biometric feature of individual, if the template is compromised, it is not possible to replace it.

Biometric template is the extracted biometric features stored in a central database or smartcard [4] which can be used to identify or verify individuals.

The biometric templates are the major target of the hackers which can be at the database level or the interconnecting channel level [4].

"Unlike password, when biometric templates are compromised, it is not possible for the legitimate user to revoke his biometric identifiers and switch to another set of uncompromised identifiers. Due to this irrevocable nature of biometric data, an attack against the stored templates constitutes a major security and privacy threat in a biometric system" [4].

To properly protect the biometric template, the protection techniques should have the following properties as outlined by Jain et al [6].

a. **Diversity**: The protected template should by no means allow cross matching in the databases. This is to ensure that user's privacy is not compromised.

b. **Revocability**: It should be possible to revoke a template when it is compromised by the hackers and reissue different one based on the biometric information.

c. **Performance:** The template protection techniques should not reduce the performance of the system.

d. **Security**: it should be computationally difficult to recover the original biometric template from the stored template. This will go a long way to ensure that hackers do not fabricate a physical spoof of the biometric treat from the stolen template.

The template protection techniques can be classified into two categories: Feature transformation and bio-cryptosystem.

Biometric Feature Transformation

Here, transformation function is applied to the biometric template and the transformed template is stored in the database [6]. The transformation function may have different characteristics and use certain parameters such as password. During verification, the verification feature set is equally transformed in the same way as the enrolment template and the comparison of the fingerprint takes place in the transformed space [14]9). This category can be divided into two: Non-invertible transform and Salting

Non-invertible transform

This category usually applies a one-way function to the unprotected template in such a way that it will be computationally difficult to reverse the protected template even when any of the parameters of the transforms are stolen or revealed [15].

This technique provides better security than Salting since it is very difficult to recover the original biometric template even if the template is compromised [6].

Hashing technique is used in password based authentication system; in this case password is hashed and stored in the database on the process of enrolment. Then during verification, the user also enters the same password and it is hashed and compared with the existing password.

It will be very difficult to recover the original password even if the exact transformations as well as transformed password are known since the transformation is non-invertible in the cryptographic point of view [15].

In the same way, it can be applied in fingerprint. Instead of storing the template of the fingerprint, the hashes of the template should be stored; then during verification, the verification feature set is also hashed and compared in the non-invertible transform space. But significant difference exists between password and fingerprint. "Passwords are exactly the same during different authentication attempts, but fingerprint image at different acquisitions (different verification attempts) are never identical, and this prevents the same hash to be obtained" [15]. Therefore, matching in the non-invertible transform space is big problem. Recovering the correct alignment between the two fingerprints: the template and the query feature set is a major problem in comparing hashed fingerprint templates [15]. One method to solve this problem is to pre-align the feature set before the transformation (e.g. registering them with respect to the core point).

Salting

In this approach, biometric features are transformed using a function defined by a user-specific key or password. The transformation is invertible to some extent, therefore the key need to be securely stored or remembered by the user and present it during authentication [6]. The need for additional information in form of key increases the entropy of the biometric template, and therefore, makes it difficult for hackers to guess the template. The Entropy of biometric template is a measure of the number of different identities that are distinguishable by a biometric system [6]. In this approach multiple templates can be generated for the same user (diversity) by using different keys since the key is user specific. Again if the template is compromised, it can be replaced by generating new template (revocability).

Biometric Cryptosystem

These techniques were originally designed for the purpose of either securing a cryptographic key using biometric features or directly generating a cryptographic key from biometric features [6]. They can also be used as a means of biometric template protection. Here, some details about the biometric template are stored in the database. These details are known as helper data; therefore, biometric cryptosystem is also referred to as helper data-based method. This technique can be further classified into two categories: Key generation and Key binding.

Key-Binding Biometric Cryptosystem

In, this approach, a cryptographic and an unprotected fingerprint template are bonded together within a cryptographic framework to generate the helper data. It is computationally difficult to decode the key or the template from the helper data without the knowledge of the user's fingerprint data. The helper data is usually obtained associating the enrolment template with codeword obtained from an error correcting code using the key as the message. A codeword recovered from a feature set that is similar but not identical to the template is affected by a certain amount of error correction code, the exact key is recovered from the codeword that contains some errors. If the correct key is recovered, it means that the feature set and the protected template result in a match [15].

Key Generation Biometric Cryptosystem

A key is derived directly from the biometric signal in this approach. The major advantage is that there is no need for user-specific keys or tokens as required by 'Biometric Salting approach'. But the problem with this approach is that it is very hard to generate key with high stability and entropy.

Experimental Evaluation

Performance Evaluation

It is obvious that fingerprint biometric system will never produce error-free recognition results. However, with proper instruction and guidance on how to position fingertip during the enrolment process, the error rate can be reduced to minimal level. To determine the performance of any system, evaluation has to be carried out.

To evaluate the performance of the system, fifty (50) fingerprints of the students of university of Greenwich were scanned (enrolled). During the enrolment, instruction on how to place their fingertips on the scanner was given to them. This was done to ensure that each student positions his/her fingerprint correctly before the scanner captures and extracts the template. The fingertip of each student used during the enrolment process must be the fingertip to use when taking Attendance. The extracted template and other details such as name of the student and email address of the student were stored in database (MYSQL) during enrolment process. On the process of taking attendance, the extracted template is compared with the template stored in the database; if matched, attendance will be taken. Some students fingerprint were not extracted at the first attempt due to incorrect positioning of the fingertips.

The **Digitalpersona Fingerprint Reader** was used to capture the fingerprint image and to extract the template. DigitalPerdona is a company that sales fingerprint reader and the SDK that helps the application to capture and extract the template.

In other to determine the performance of the system, two error rates were used- The False Acceptance Rate(FAR) and The False Rejection Rate(FRR) which are commonly used to measure the performance and accuracy of biometric system. The False Acceptance Rate is the probability that student not enrolled will be identified when taking attendance while False Rejection Rate is the probability that enrolled student will be rejected when taking attendance.

During the evaluation, there was no false acceptance (student that was not enrolled was not identified during attendance). Few false rejections were identified, that is some students that were enrolled into the system were not identified during attendance. The false rejection might be due to improper positioning of the student fingertip during the enrolment process.

During the evaluation process, we discovered that a student can be enrolled more than once with the same finger depending on how the student positioned his/her finger during the enrolment. This happens because the scanner extracts the particular side of the fingertip placed on the scanner; the extracted template is encrypted and stored in the database. So, during attendance, the student must also position his/her fingertips the way it was done during the enrolment stage. We also tested the system with finger toes (leg) and discovered that the scanner also recognized it as it does for fingertip (hand). So finger toes can also be used to recognize individuals. This will help if the person lost his/her fingers due to one problem or the other.

The fifty (50) students used to evaluate the project were from different levels in the university. Level 1 (year one students), level 2 (year two students), level 3 (year three students) and level 4 (masters students). Success rate obtained during the process was up to 93%. The result is shown in the table 1 below:

Table 1: Degree of success and Failure

Level	Success Rate (%)	Failure Rate (%)
1	85	15
2	95	5
3	95	5
4	100	0

From the table shown above, it implies that year one students had the lowest success rate with 85%; this might be due to incorrect positioning of finger. Second year students had 95% success rate, third year students had 95% success rate while master's students had the highest level of success rate with 100%.

The Bar chart shown below indicates the comparison:

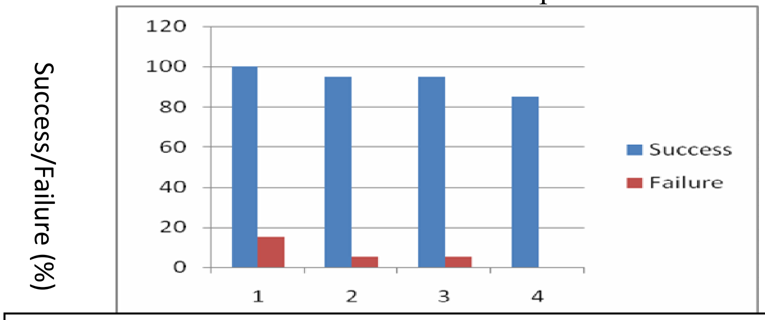


Figure 2: Bar Chart showing the comparison of success and failure rate

In comparison to the existing system where a lecturer has to print the attendance list and each student signs on the paper during attendance, the Automated Fingerprint System is more accurate because, the student has to be around during the attendance. In the paper type a student can sign for another student, thereby not achieving the aim of taking the attendance. The system (Attendance system using fingerprint biometric) is also faster because, in the paper type, lecturer has to devote another time to enter the attendance record into the existing system after taking the attendance. The lecturer can also make mistake of not recording attendance for student that was in the class or record present for student that was not in the class. But for the fingerprint biometric system, as student places his/her fingerprint on the scanner, the attendance is taken immediately and details of the student submitted to the database.

Security Evaluation

With the increase in the use of biometrics, there is concern about the privacy and security of the biometric template stored in the database.

Biometric system involves Enrolment and Identification process. The system enrols a student by storing his/her biometric feature (Template) in the database. Then the stored template is queried against the template generated during identification process. If matched, the student will gain access to the system. Also employees are registered in the system. Before they login to the system to take student attendance, their own finger prints must first be scanned and if the generated template matches with the stored template, the staff will gain access to the system to take attendance.

Protecting the stored fingerprint template is very important as individual has unique features which when compromised cannot be recovered. If the student templates which are stored in the database during the process of enrolment are not properly protected, it can result to imposter misusing the template for their own gain. Therefore, it is paramount to protect the privacy of students when they are enrolled into the system.

It is obvious that web application is exposed to both good and bad intended users. If bad intended user gain access to the system, they can also attack the system thereby preventing the intended user having access to the application.

To evaluate the security of the system, we will look at how secured is the generated template that are stored in the database during enrolment.

"A biometric template is a digital representation of an individual's distinct characteristics, representing information extracted from a biometric sample. Biometric templates are what are actually compared in a biometric recognition system. Templates can vary between biometric modalities as well as vendors"[18].

Our initial objective was to concatenate the biometric template with the student username before submitting it to the database. But when we discovered that the template was encrypted with very large digits, we decided to submit only the encrypted template. When viewed the submitted template in the database, we noticed that the template was submitted as **BLOB**. Blob is a data type used to store very large object in the database. This implied that even if imposter gained access to the template, it would take the person ages to manipulate a false fingerprint that could generate the same template with the one stored in the database. The imposter never succeed in comprosing the template..

In view of that, the system is highly secured and the privacy of students are certain, since the template submitted to the database is encrypted and the encrypted template is very large digits generated from the fingerprint.

Furthermore, since web application is vulnerable to so many errors such as SQL Injection and Buffer overflow, certain measures were also adopted to ensure that the application is secured from those vulnerabilities. For instance, to reduce the chances of the system experiencing buffer overflow, both client and server validation was properly done. It is true that server side validation reduce the performance of the system compared to client side validation; but in a system like this, where security is more important, it had to be done.

Future Work / Recommendation

During enrolment process, student scans his/her one fingerprint which is encrypted and submitted to the database along with the student's details. The fingerprint used during enrolment must be the fingerprint to use when taking attendance. If the student is identified; he/she will be recorded present. Identifying student with only one fingerprint is not sufficiently enough. The system can be improved by scanning and encrypting together two different fingerprint of each student during enrolment so that while taking attendance, they will also scan their two fingerprint. If identified, the student will be recorded present.

The security of the system can also be improved by concatenating the student username (email address) with the extracted template so that even if someone gains access to the database, he/she will not be able to differentiate the template from the username.

The template protection scheme is not perfectly enough in ensuring strong security; it does not meet the requirement of revocability. It should be possible to revoke a template when it is compromised by the hackers and reissue different one based on the biometric information.

Furthermore, another enhancement area is using multi-modal biometric system (using two or more biometric feature) to identify staff or student. The system identifies student or staff with only fingerprint biometric feature; incorporating other biometric features such as face, voice iris or retina will definitely enhance the performance and security of the system.

Again due to time constraint, we could not carry out detailed research on how the template is extracted. Each vendor of the biometric tools has their mathematical model that extracts the template from the fingerprint image. Developers can also manipulate their own mathematical equation (e.g. polynomial) so that when the template is generated, the equation developed by the developer will convert the template to different digits. This will make template different across different applications using the same vendor.

Conclusion

The advantages of biometric recognition system are quite enormous. Users cannot lose their biometric features even at old age and is very hard to forge another person's biometric feature.

Ethical issues have been raised about the use of biometric system, but due to difference threats around the globe such as security, impersonation, illegal immigration identity theft and fraud etc, it is very important to implement biometric system for better identification and verification. Any system is vulnerable to attack, including biometric system especially when deployed to the web where everyone can have access to it. This paper suggested different mechanisms to handle the possible attacks on the web and enumerated different means to adopt in ensuring that user's fingerprint template is properly secured and privacy protected.

In this paper, performance and security evaluation of biometric web based application has been carried out successfully. From the report, using fingerprint biometric recognition as a means of authentication is a welcome idea since this has shown high level of performance of the system and security of information stored in the database.

From the experiment carried out, automating Student Attendance Monitoring System using biometric technology greatly improves the performance of the system. Someone will not be able sign for another student during attendance since the system must identify the person using his unique fingerprint. Furthermore, the system has eliminated the paper work used to sign attendance during lectures by automatically submitting student details into the database as the student places his finger in the scanner. Finally, the work has touched on the usual neglected problem of privacy and security of biometric features. High level of template security has been achieved, since the generated fingerprint feature of students are encrypted before submitting to the database. This entails that even if hackers gain access to the database, it will not be easy for them to manipulate a fake finger that can match the stored template in the database.

References

[1] Dror, E. & Shaikh, A., 2005. *Face Recognition Technology: Cognitive Considerations in System Design,* s.l.: United Kingdom Passport Services(UKPS) Technical Report.

[2] Fry, J. & Dunphy, A., 2009. *Biometric Student Identification: Practical Solutions for Accountability and Security in Schools.* [Online] Available at: http://www.identimetrics.net/articles/Practical_Stu_ID_for_schools.pdf [Accessed 7 June 2013].

[3] Gorodnichy, D., 2009. Evolution and evaluation of biometric system. *IEEE symposium on computation inteligence for security and defence applications.*

[4] Gudavalli, M., Raju, S. & Kumar, K., 2012. A Template Protection Scheme for Multimodal Biometric System with Fingerprint, Palprint, Iris and Retinal Traits. *ACM,* pp. 102-106.

[5] Hsiung, T. & Mohamed, S., 2011. Performance of Iris Recognition using Low Resolution Iris Image for Attendance Monitoring. *International Conference on Computer Applications and Industrial Electronics.*

[6] Jain, A., Nandakumar, K. & Nagar, A., 2008. Biometric Template Security. *EURASIP*

urnal on Advances in Signal Processing, pp. 1-17.

[7] Jain, A., Prabhacker, S. & Ross, A., 1998. *Biometric-Based Web Access,* s.l.: ansactions of the Institute of British Geographers.

[8] Jain, A., Rose, A. & Prabhakar, S., 2004. An Introduction to Biometric Recongnition. *EEE Transactions on Circuits and Systems for Video Technology,* 14(1).

[9] Jain, A., Ross, A. & Uludag, U., 2005. *Biometric Template Security: Challenges and Solutions.* Antalya,Turkey, Preceedings of European Signal Processing Conference(EUSIPCO).

[10] Kadry, S. & Smaili, K., 2007. A Design and Implementation of a Wireless Iris Recognition Attendance Management System. *Information Technology and control,* 36(3), pp. 323-329.

[11] Kawaguchi, Y. et al., 2010. *Face Recognition-based Lecture Attendance System,* Kyoto University: Academic Center for Computing and Media Studies.

[12] Khaw, P., 2002. *Iris Recognition Technology for Improved Technology,* s.l.: SANS Institute.

[13] Lee, H. & Gaensslen, R., 2001. *Advances in Fingerprint Recognition.* 2nd ed. s.l.:CRC Press, Taylor and Francis Group.

[14] Maiwald, E., 2004. *Fundamentals of Network Security.* s.l.:McGraw-Hill Technology Education.

[15] Maltoni, D., Maio, D., Jain, A. & Prabhakar, S., 2009. *HandBook of Fingerprint Recongnition.* 2nd ed. s.l.:Springer.

[16] Mishra, R. & Trivedi, P., 2011. *Student Attendance System Based On Fingerprint cognition and One-to-Many Matching.* [Online] Available at: http://ethesis.nitrkl.ac.in/2214/1/thesis.pdf
[Accessed 3 July 2013].

[17] Mohammed, A.-A. & Kameswari, J., 2013. Web-Server based Student Attendance System using RFID Technology. *International Journal of Engineering Trends and Technology,* 4(5), pp. 1559-15563.

[18] Pau, V., 2008. *Biometrics.* [Online] Available at:
http://www.scribd.com/doc/23636365/biometrics- eminar-report
[Accessed 6 September 2013].

[19] Ratha, N., Chikkerur, S., Connell, J. & Bolle, R., 2007. Generating Cancelable Fingerprint Templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 29(4), pp. 561-572.

[20] Ratha, N., Connell, J. & Bolle, R., 2001. Enhancing Security and Privacy in Biometric-based Authentication Systems. *IBM Systems Journal.*

[21] Saraswat, C. & Kumar, A., 2010. An Efficient Automatic Attendance System using Fingerprint Verification Technique. *International Journal on Computer Science and Engineering,* 2(2), pp. 264-269.

[22] Shoewu, O. & Idowu, O., 2012. Development of Attendance Management System using Biometrics. *The Pacific Journal of Science and Technology,* 13(1), pp. 300-307.

[23] Teodoro, N. & Serrao, C., 2011. *Web Application Security:Improving Critical Web-based Applications Quality through in-dept Security Analysis,* s.l.: IEEE.

[24] Watson, S., 2008. *How Fingerprinting Works.* [Online] Available at: http://science.howstuffworks.com/fingerprinting1.htm [Accessed 23 July 2013].

[25] Zhang, D., Song, F. & Xu, Y., 2009. Advanced Pattern Recognition Technologies with Applications to Biometrics. s.l.: Book News Inc.