ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 12 , December 2019

Development of a Secured Database System for Higher Educational Institutions in Nigeria

Oladimeji S.A., Agbakwuru O.A., Opara C.C., Etim Emmauel

Department of Computer Science, Federal Polytechnic Nekede, Owerri, Imo State.
Department of Computer Science, Imo State University Owerri, Imo State.
Department of Computer Science, Federal Polytechnic Nekede, Owerri, Imo State.
Department of Computer Science, Abia State Polytechnic, Abia State.

ABSTRACT: University information systems have become ideal targets for hackers; this is because the systems contain sensitive personal data as well as abundance of intellectual property from researchers. In many ways, colleges and universities experience the same data security breaches major corporations do. Internal frauds had been attributed to major database attacks in the recent time. While enterprise systems are set up to meet business needs, university systems are designed on the principles of free information exchange and to accommodate diverse user populations. The motivation of this research is as a result of several attacks posed on higher institution databases due to weak authentication system. The aim of this dissertation is to design a multifactor authentication security system where a user can enter unique username, password fingerprint and face-print in order to have access into database. The structured system analysis and design methodology (SSADM) and OOAD is used to design the application. C# and Visual Studio 2015 .Net framework 4.0 IDE for building the application while the database backend is Microsoft SQL server 2008 R2. The result is that the new system compulsorily prompts for username, password, fingerprint and face capture in order to gain access into the institution's database system.

KEYWORDS: Data Breach, Fingerprint, Hackers, Intellectual Property, MFA etc.

I.INTRODUCTION

Organizations are becoming more concerned about data security, especially as the intrinsic value of our data continues to increase. However, database security often gets overlooked. Managing organizational assets such as data, as well as overall information security concerns, are two of the key technology areas having a large affect on companies today. Although it is often difficult to put an exact price tag on the data we store, we do know data is an extremely valuable asset, and the compromise and/or exposure of such information can cause significant damage to business and company reputation. As a result, a security strategy needs to be developed to address information security risks, including data security. The intent of multi-factor authentication (MFA) is to provide a higher degree of assurance of the identity of the individual attempting to access a resource, such as physical location, computing device, network or a database. MFA creates a multi-layered mechanism that an unauthorized user would have to defeat in order to gain access. Multi-factor authentication is one of the most effective controls an organization can implement to prevent an adversary from gaining access to a database, device or network and accessing sensitive information. When implemented correctly, multi-factor authentication can make it significantly more difficult for an adversary to steal legitimate credentials to facilitate further malicious activities on a network. Due to its effectiveness, multi-factor authentication is one of the essential security measures to mitigate Security Incidents. The Australian Cyber Security Centre (ACSC) recommends that multi-factor authentication is implemented for users using remote access solutions, users performing privileged actions and users accessing important (sensitive or high-availability) data repositories (acsc.gov.au) Using multi-factor authentication provides a secure authentication mechanism that is not as susceptible to brute force attacks as traditional single-factor authentication methods using passwords or passphrases[1].

When the subject of hacking and database attacks in colleges and universities arises, people tend to think of students hacking into the network to adjust their grades to hide bad performance from their parents and future employers. However, recent database attacks at several universities have shown that student grades are not the main target. Chabrow (2015) explains that university systems are seen as ideal targets for hackers since the systems contain sensitive personal data as well as an abundance of intellectual property from researchers [5]. Chabrow describes the cybercriminals infiltrating the institutional systems as well-funded and highly skilled perpetrators who have become aggressive in their attacks. Nick Bennett, senior manager at Mandiant, told Reuters that cyber-attacks similar to the one at Penn State in 2015 are now real and that no company or organization is immune. The hacks are sophisticated, difficult to detect and often linked to international threat actors. Colleges and universities have large amounts of data and are difficult to secure [2]. Hackers have used several methods to hack higher educational institutions in the last couple of years from hacking and malware to skimming hardware and insider attacks [5]. According to information from the massive database maintained by Privacy Rights Clearinghouse, about 30 educational institutions experienced data breaches in 2014 alone. Five of the 30 higher educational institutions actually had larger data breaches than the notorious Sony Hack [6]. This research examines database targets at universities, types of breaches to access the data, several recent university breaches and proffers solutions to prevent such attacks.

Why Attacks on Educational Institutions?

Educational institutions are seen as soft target for attackers according to Tyler Shields, a security analyst at Forrester Research(Roman,2014). Shields, who previously worked for Rochester Institute of Technology in New York, states that the culture of academic institutions is one of open communication and collaboration among students, staff, visiting Professors, faculty members and research groups. The system users are highly mobile and are accustomed to networking and accessing the database whenever and wherever they are and on any device. The academic culture of openness and unencumbered access to content and data makes college and university databases extremely difficult to secure. The lax security allowing open access and the presence of cutting-edge academic research and content on the database make educational institutions an attractive target for attackers.

In an article in InsideHigherEd.com [6], Chad Holmes, a chief security strategist with FireEye, makes similar statements about the culture of higher education and difficulties of securing their systems. Like Shields, Holmes said that it is the nature of universities which makes the database tougher to secure. Holmes continues that universities are more difficult to secure than companies and government agencies due to the fact that faculty members and students demand more control of their data than do employees of companies and government agencies [3].

Research Questions

In an attempt to achieve the research objectives, this dissertation aims to answer the following research questions and sub-questions:

RQ 1) What are the potential security threats to Higher institution educational databases?

i. What are the potential collusion and non-collusion threats to databases?

RQ 2) What method can be used to support secure authentication of users in educational databases?

ii. How can the challenge question approach be used for authentication of users ?

RQ 3) How does the usability of the proposed multifactor authentication method influence the security of database?

RQ 4) How does the proposed authentication method influence security threats? Etc.

RQ 5) How can the proposed system be used to take audit of every access to the database?

II. SIGNIFICANCE OF THE SYSTEM

This study is significant in the sense that, considering the risks and university culture, the number of potential university database attack scenarios is almost unlimited. Attackers have already targeted both students and staff records. Major attacks occurred as a result of internal collaboration. Insider attack is common in most of educational institutions. Data compromised in higher institutions breaches extend far past grades; personal and financial data are abundant at all institutions, and sensitive research data are stored at many large universities. The most common types of data breaches occurring in college and university systems are hacking and malware, unintentional disclosure, and portable device breaches. The study is significant due to the risks posed to our database. If the system is implemented it will eliminate insider and outsider attacks to our educational databases and it will make students more serious about their studies having known that there is no way one can change or alter grades in the database. Finally the system will monitor every access to the database to ascertain who does what, where and at what time?

III. LITERATURE SURVEY

Database Attacks in Higher Institutions

Grama et al, 2014 [6] opined that the categories of database attacks that are most common in higher education are hacking or malware, unintended disclosure, and portable device breaches. Researchers at the ECUCAUSE Center for Analysis and Research (ECAR) determined that 36% of breaches were committed by hacking or malware, 30% by unintended disclosure, and 17% by portable device breaches.

According to Njenga, the increase in the number of cyber attack incidents is partly the result of the availability of online information about how to perpetrate attacks [9]. In addition, secure software development in Africa has been an issue as developers focus more on "functional" coding than on "secure" coding, he said. Among the continent's most recent targets were Zimbabwe's National University of Science and Technology and the Harare Institute of Technology [11].

According to a report in the online Chronicle, the institutions' websites were hacked and the servers hosting both website and emails were temporarily out of control. Other incidents, with motives ranging from fraud to political or protest action and ransom, have been reported at universities in Algeria, Egypt, Morocco, Kenya, Nigeria, Botswana, Uganda, Ghana and South Africa [11]

According to the Africa Cyber Security Report 2016, African countries lost at least US$2 billion in cyber attacks in 2016. The report is published by Serianu, an information technology services and business consulting firm, in conjunction with United States International University-Africa's Centre for Informatics Research and Innovation. Despite this, only eight African countries feature in the top 50 countries in cyber security, according to the Global Cyber Security Index. They include Mauritius (at 6), Egypt (at 14), Rwanda (at 36), Tunisia (at 40), Kenya (at 45), Nigeria (at 46), Morocco (at 49) and Uganda (at 50). Cyber security expert and co-founder and chair of AfricaHackOn – East Africa's premier technical computer security collective – Bright Gameli Mawudor told University World News that part of the problem is that African universities are not proactive about cyber threats [11]

Unfortunately, we now live in an environment where no computer network can ever be completely, 100 percent secure, a Penn State representative shared [12]. The PSU representative further stated that on the average day the PSU university computer system repels more than 22 million overtly hostile cyber-attacks from around the world. Colleges and universities need to have plans in place to prepare and to react to data breaches.

Beaudin (2015) makes several recommendations as to how colleges and universities can prepare for a data breach and react to a breach when one occurs. Preparation for a database breach is an important part of an overall information security plan. Plans for reacting to a breach acknowledges that breaches are likely to occur and details in advance how to mitigate damage and costs due to the breach. Information technology administrators need to ensure that information technology best practices and security policies are adopted and communicated [14].

Personnel handling data need to know how data are collected, stored, and protected. Responsible personnel need to know their role in incident response in case of data vulnerability (Beaudin). All people on campus handling data need to know their role in data safety, including administrators, faculty, staff, researchers, and students [14]. Practices and policies include password, authentication, access, and portable devices issues. Communication is a crucial element of a successful plan – everyone needs to know his or her particular role in preventing a breach and reacting to a breach. Personnel can introduce Biometric technology or encrypt sensitive data. The two main means of reacting to a data breach are timely notification and free fraud protection [5]. Responsible administrators need to inform affected employees and students once a breach is detected and compromised data identified. Free fraud protection is typically offered to identify victims and the cost is a major expense of the data breach.

Recent Database Attacks

- Guy Cormier, president and CEO of Desjardins Group, announced in June that an employee improperly accessed and shared the information of 2.7 million individuals and some 173,000 businesses [13]. (Paul Chiasson/Canadian Press)

- An employee with "ill-intention" at Desjardins Group collected information about nearly three million people and businesses and shared it with others outside the Quebec-based financial institution [13].

- The data breach affects around 2.7 million people and 173,000 businesses, more than 40 per cent of the co-operative's clients and members[13].

- The leaked information includes names, addresses, birth dates, social insurance numbers, email addresses and information about transaction habits.

- Desjardins CEO and president Guy Cormier said the security breach was not the result of a cyberattack, but the work of an employee who improperly accessed and shared the information [13].

- The security breach is among the biggest in Canada to come about internally, as opposed to an external cyberattack, in recent years.

- The Bank of Montreal and the Canadian Imperial Bank of Commerce both suffered data breaches last May 2019 [16]

- Equifax announced in 2017 that a massive data breach compromised the personal information and credit card details of 143 million Americans and 100,000 Canadians.

- In August, some 20,000 Air Canada customers learned their personal data may have been compromised following a breach in the airline’s mobile app [13]

- In the past three years, millions of consumers have been affected by data breach against companies including British Airways, Uber, Deloitte, Ashley Madison and Walmart [15]. (Christopher Reynolds, The Canadian Press)

Summary of Selected Cases of Database Attacks in Higher Educational Institutions

Data Breaches	Date	Records Breached	Type of Breach	Type of Target
University of Maryland	19/02/2014	309079	Hacking or malware	Educational Institutions
North Dakota University	06/03/2014	290780	Hacking or malware	Educational Institutions
Butler University	30/06/2014	163000	Hacking or malware	Educational Institutions
Indiana University	26/02/2014	146000	Hacking or malware	Educational Institutions
Riverside Community College	16/06/2014	35212	Unintended disclosure	Educational Institutions
Iowa State University	22/04/2014	29780	Hacking or malware	Educational Institutions

University of California - Santa Barbara	**07/08/2014**	**2100**	Hacking or malware	Educational Institutions
Douglas County School District	16/07/2014	Undisclosed	Portable device	Educational Institutions
Barry University	10/01/2014	Undisclosed	Hacking or malware	Educational Institutions
Zimbabwe's National University of Science and Technology	2016	Undisclosed	Hacking or malware	Educational Institutions
Harare Institute of Technology.	2016	Undisclosed	Hacking or malware	Educational Institutions
University of Lagos	2016	Undisclosed	Hacking or malware	Educational Institutions
Federal Polytechnic Nekede, Owerri.	2010	Undisclosed number of records	Hacking or malware	Educational Institutions

IV.METHODOLOGY

At this stage the researcher used both primary and secondary methods of data collection. First, data were gathered through experience, interview, questionnaire and periodicals. Some materials are collected from journals, texts book and research papers gathered from libraries and Internet.

A. Analysis of the Present System

The existing system of securing database in higher institutions is purely " use of username and password" to access database. Database of higher educational institution has the following units of operations:

- Candidate buying the application Form and Scratch cards. Forms can be purchased from the designated banks.
- Candidate proceeds to online registration; this is done through filling of forms that contains the necessary information about the student. This system helps keeping the student's profile and allows the student to check and re-check admission status as when necessary.

- With the use of password and username, It also helps the student in re-ensuring safe accounts though not reliable.
- Candidate's form is processed by the administrator and the form status is uploaded for candidate to access whenever the admission is out.

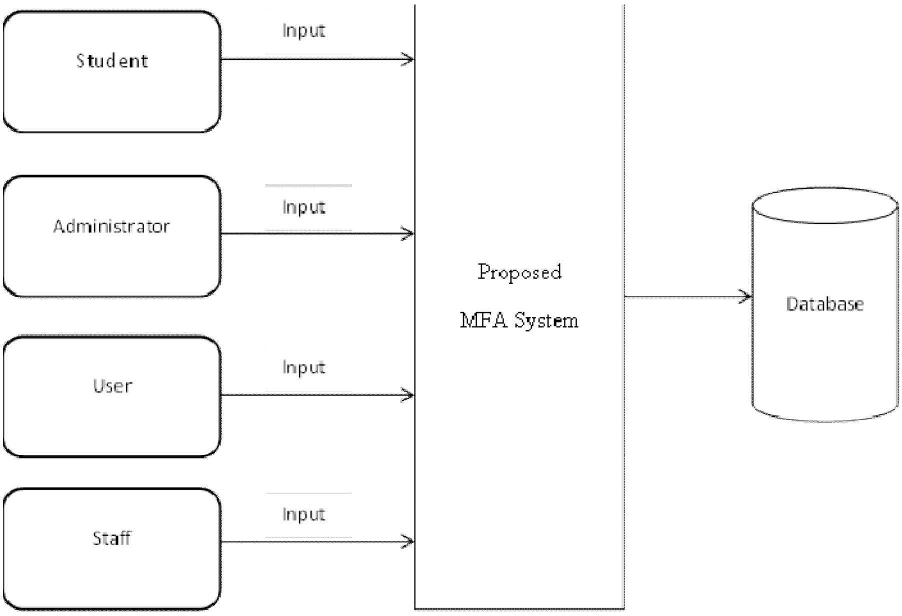
B. Weaknesses of the Existing System

Shoulder Surfing allows the attacker to physically view the password as it is typed so he can remember it for later use. Another common mistake made by users is to write their password down on a piece of paper and keep it in plain view of others. Someone wishing to falsely log on to a network needs only look to these sheets of paper for a password to use. Weak password is common problem in many organizations. Lack of Identity Check is another one, supplying a correct password does not prove an individual is who she claims she is. Also, we may experience internal attacks such that somebody within the organization uploaded unqualified candidates for admission. This is easy to do in as much as nobody is check-mating the administrator. The existing system has no auditing characteristics.

C. Systems Design

The program is designed to take care of the respective tasks that constitute the biometric information security system and its implementation, the program design is based on the input and output specification to facilitate easy coding, testing, debugging. The database used is MySQL as back end, while the programming language used is C sharp(C#), and its execution and explanation will be on pieces with Windows operating platform. After the documentation of the new system, problematic area and future requirement by the system analyst, the next procedure becomes the design of the new system. The system is concerned mainly with the User-ID/password authentication, Fingerprint verification, Face detection and recognition and Record-based Verification. The system to be designed is to be judged based on the following performances:

i. Achieving its aim (strong authentication)
ii. Timeliness
iii. The capacity of the system to handle database attack.
iv. The quality of security it can provide
v. Efficiency of the system in terms of security of database against attacks
vi. Reliable security and control mechanism
vii. Accuracy of the system
viii. Audit Trail
ix. Feedback mechanism



1) Figure 4.1: Architecture of the Proposed system

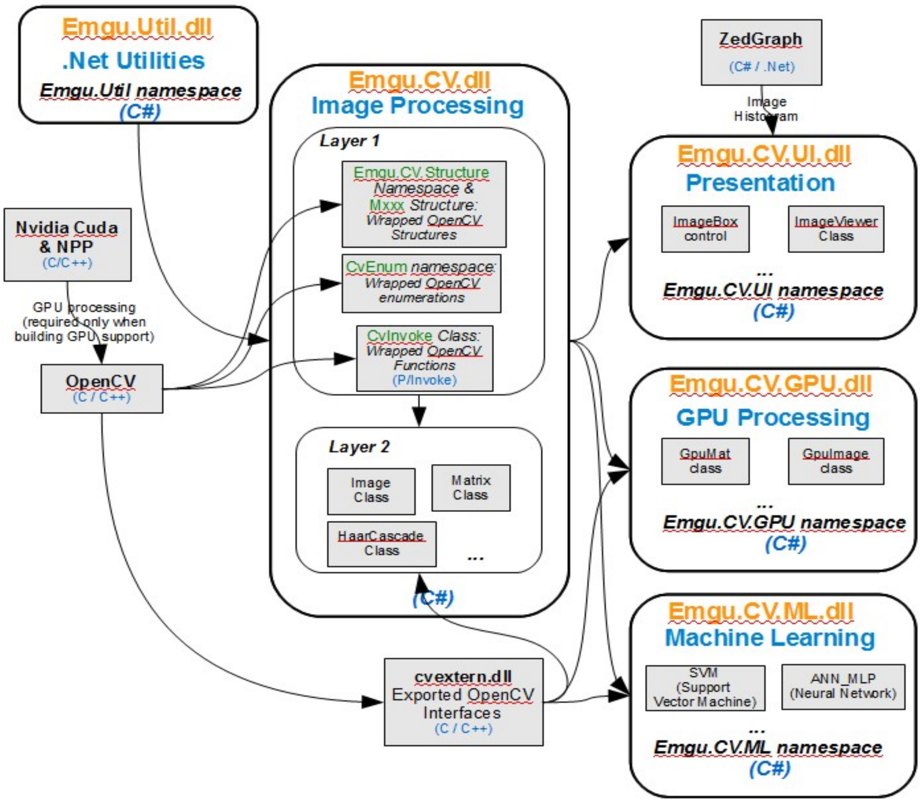


Figure 4.7 EmguCV Diagram.(www.emgucv.com)

V. EXPERIMENTA RESULTS

Based on the results of training and testing related to face recognition using Principal Component Analysis (PCA) and EmguCV, the following data are obtained:

Test Result at 50 cm Distance

In this test, the distance used between the object and the camera is approximately 50 cm. The data obtained are shown in table 1 below.

Table 4.1 Face Recognition at 50 cm Distance.

NO	Recognition Result		
	Name	*Accuracy*	*Time*
1	Person 1	85	0.96
2	Person 2	88	0.97
3	Person 3	90	0.89
4	Person 4	91	0.99
5	Person 5	89	1.09
6	Person 6	90	1,08
7	Person 7	91	1.08
8	Person 8	88	1.08
9	Person 9	89	1,05
10	Person 10	90	0.90
	Average	**89.1**	**1.009**

Based on the data contained in the table above, it can be analyzed that holistically, the results of the introduction using PCA method with threshold used between 0.1 to 1, shows recognition accuracy is about 89.1 with the required time is 1.009 seconds.

Test Result at 100 cm Distance

The next test is facial recognition at a distance of 100 cm. Based on test, the results and training obtained data is shown in table 2 below.

Table 4.2. The Result of facial recognition on 100 cm distance.

NO	Recognition Result		
	Name	*Accuracy*	*Name*
1	Person 1	87	0.98
2	Person 2	86	1.89
3	Person 3	89	1.89
4	Person 4	88	1.88
5	Person 5	87	0.98
6	Person 6	88	1.009
7	Person 7	86	1.078
8	Person 8	85	1.098
9	Person 9	88	0.987
10	Person 10	87	1.098
	Average	**87.1**	**1.289**

Based on the data shown in table 4.2 above, we can analyze that the average level of accuracy of the facial mask at 100 cm distance is 87.2 with computation time is about 1.289 seconds.

Test Result at 150 cm Distance

The last test is a test at a distance of 150 cm, based on the test results obtained data as shown in table 4.3 below.

Table 4.3 Facial recognition result on 150 cm.

NO	Recognition Result		
	Name	*Accuracy*	*Name*
1	Person 1	86	0.788
2	Person 2	84	1.076
3	Person 3	82	1.0876
4	Person 4	85	1.0986
5	Person 5	86	0.987
6	Person 6	87	1.088
7	Person 7	85	0.879
8	Person 8	84	0.879
9	Person 9	86	1.009
10	Person 10	87	1.088
	Average	**85.2**	**0.998**

Based on the data shown in table 4.3 above, then we can analyze that the average level of recognition accuracy at a distance of 150 cm is 85.2 with a computation time of 0.998 seconds. Based on some test that has been done at 50 cm, 100 cm and 150. it can be seen that each of them has a different level of accuracy because it is influenced by many factors such as distance and background lighting. Similar things have also been done by where the distance of illumination and background greatly affect the results of the introduction. But overall the accuracy of PCA and EmguCV in face recognition in Real Time is in good category as shown in table 4.4 below.

Table 4.4 Accumulation of Face Recognition.

NO	Recognition result		
	Recognition distance	*Result*	*Time*
1	50 cm distance	**89.1**	**1.009**
2	100 cm distance	**87.1**	**1.289**
3	150 cm distance	**85.2**	**0.998**
	Average	**87.13**	**1.987**

Based on the data shown in the above table, we can conclude that the average face recognition in real time using PCA and EmguCV methods has the accuracy of 87.13 with computation time of 1.987. Compared with previous research, this research is still low on accuracy, this is caused by several factors, such as the data used is different and data retrieval techniques are also different. Here is a comparison between the results of current research with previous research.

Table 4.5 Comparison Result Face Recognition.

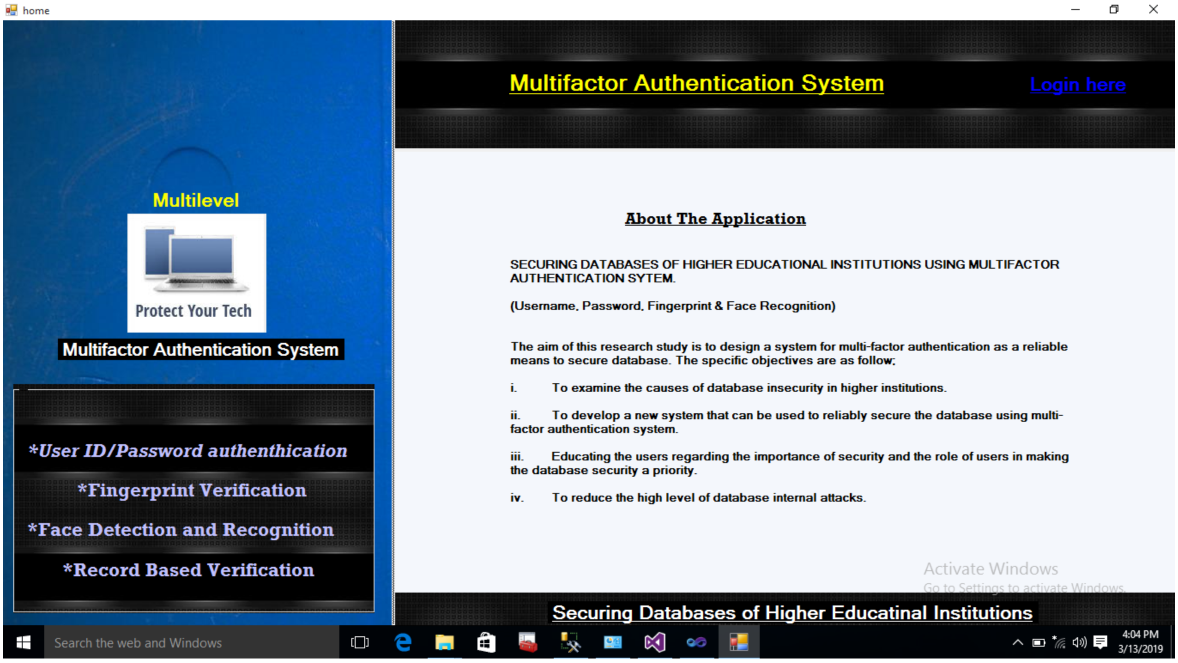
NO	Recognition Result	
	Method	*Accuracy*
1	LBP	**94.8**
2	PCA+GA+NN	**81**
3	PCA + EmguCV	**87.13**

Based on the data in the table above, we can see that PCA method has better accuracy when compared with PCA_GA + NN but still lower if with LBP. It is because the difference data are used for LBP method with PCA + EmguCV, where LBP using silent data while PCA + EmguCV uses graded image data. However, when compared to the same PCA + AG + JST using mobile image data, the PCA + EmguCV method has better accuracy

Conclusively, based on the results of the analysis and analysis as described above, it can be concluded that the PCA method combined with EmguCV is very likely to be developed to create security-based system application of image processing, with statistical and algorithm method which is simple but has a good accuracy and computation time. This research can still be combined with other methods to get more optimal results, so that it can be applied in the real world such as for absenteeism and security [14].

Input Design: This is the input designated in such a way that data validation is enhanced. It consists of the following:

i. A table for Login/Menu


home
Multifactor Authentication System
Login here
Multilevel
Protect Your Tech
Multifactor Authentication System
*User ID/Password authenthication
*Fingerprint Verification
*Face Detection and Recognition
*Record Based Verification
Securing Databases of Higher Educatinal Institutions
Activate Windows
Go to Settings to activate Windows.
Search the web and Windows
4:04 PM
3/13/2019

About The Application

SECURING DATABASES OF HIGHER EDUCATIONAL INSTITUTIONS USING MULTIFACTOR AUTHENTICATION SYTEM.

(Username, Password, Fingerprint & Face Recognition)

The aim of this research study is to design a system for multi-factor authentication as a reliable means to secure database. The specific objectives are as follow;

i. To examine the causes of database insecurity in higher institutions.

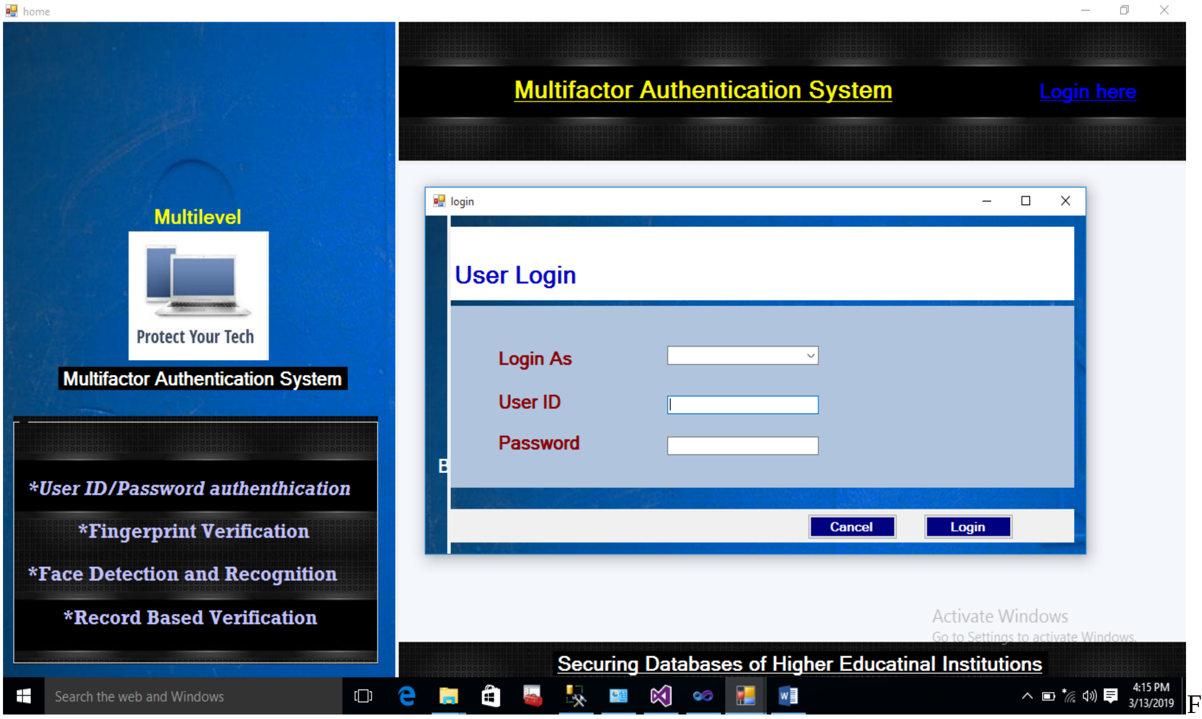
ii. To develop a new system that can be used to reliably secure the database using multi-factor authentication system.

iii. Educating the users regarding the importance of security and the role of users in making the database security a priority.

iv. To reduce the high level of database internal attacks.

Fig. 4.8 Login Picture Table

ii. Picture box for the user Login


home
Multifactor Authentication System
Login here
Multilevel
Protect Your Tech
Multifactor Authentication System
*User ID/Password authenthication
*Fingerprint Verification
*Face Detection and Recognition
*Record Based Verification
login
Cancel
Login
Securing Databases of Higher Educatinal Institutions
Activate Windows
Go to Settings to activate Windows.
Search the web and Windows
4:15 PM
3/13/2019

User Login

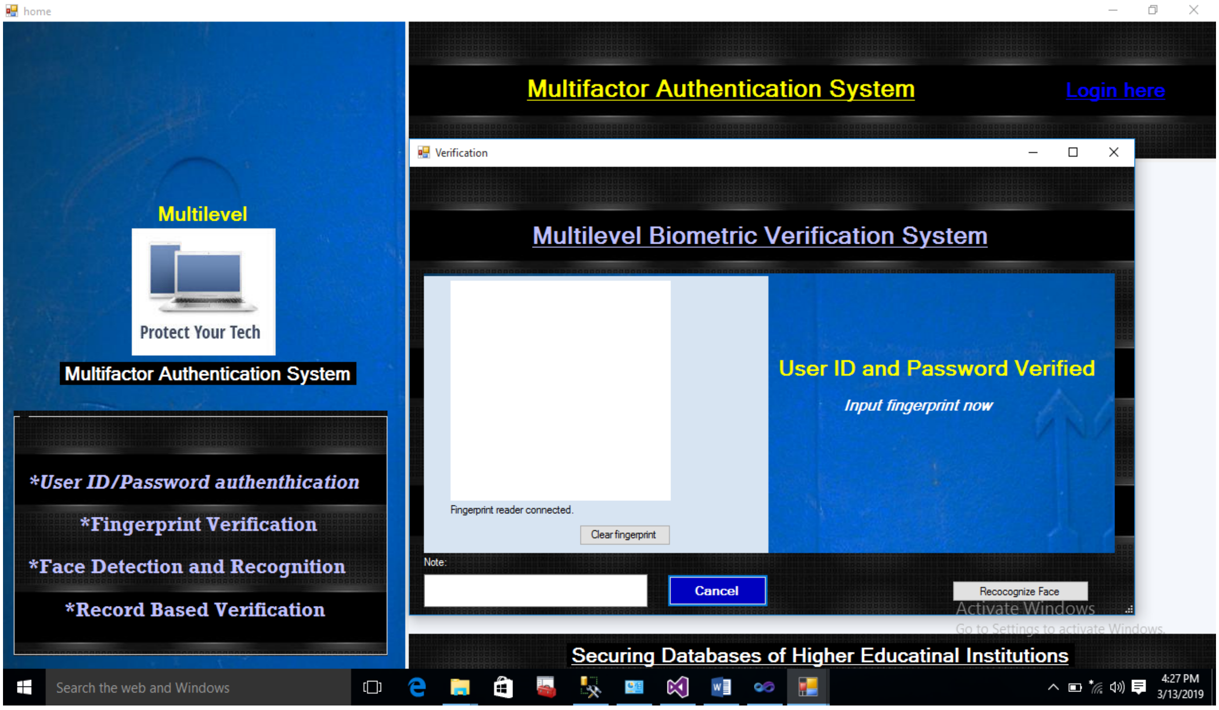
Login As

User ID

Password

Fig. 4.9 Picture box for the user Login

iii. A picture box for Fingerprint Verification


home
Multilevel
Protect Your Tech
Multifactor Authentication System
*User ID/Password authenthication
*Fingerprint Verification
*Face Detection and Recognition
*Record Based Verification
Multifactor Authentication System
Login here
Verification
Multilevel Biometric Verification System
Clear fingerprint
Note:
Cancel
Recocognize Face
Securing Databases of Higher Educatinal Institutions
Search the web and Windows
4:27 PM
3/13/2019

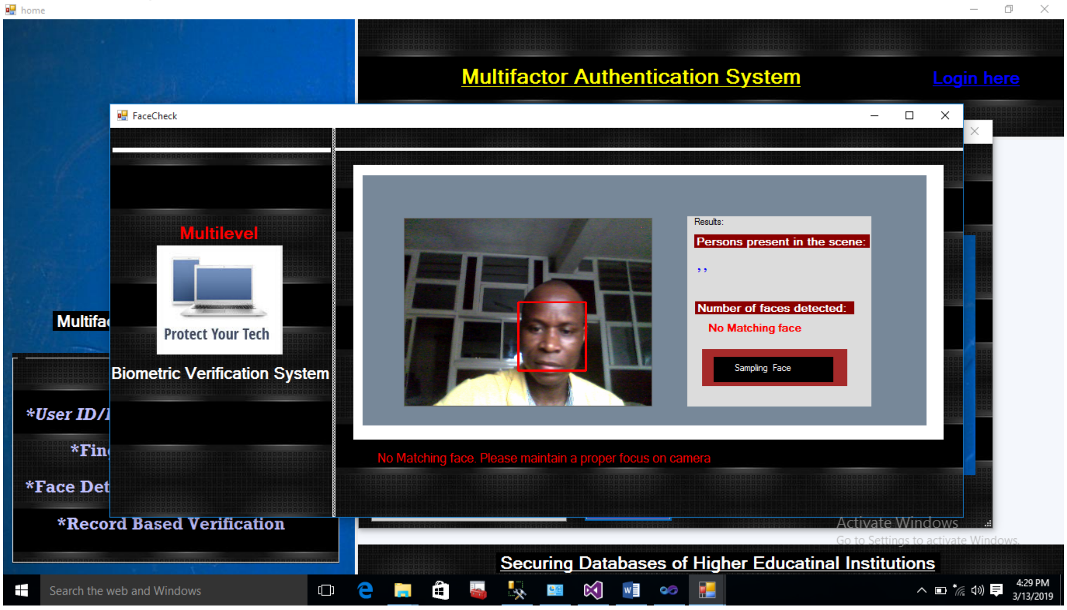
User ID and Password Verified

Input fingerprint now

Fingerprint reader connected.

Fig. 4.10 Fingerprint Verification

iv. Face Recognition Picture box

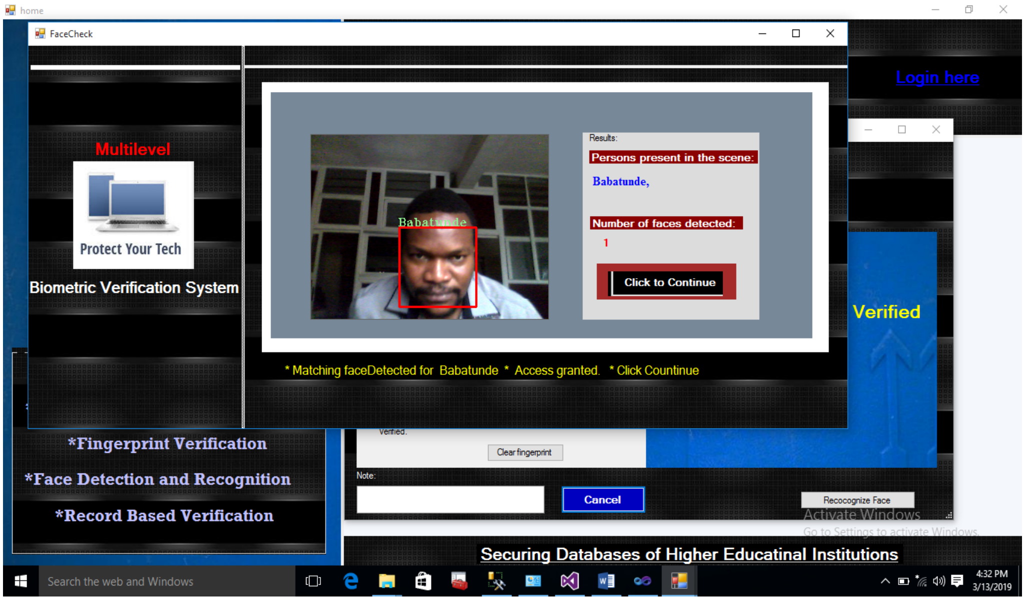

home
Multifactor Authentication System
Login here
FaceCheck
Multilevel
Protect Your Tech
Biometric Verification System
*User ID/
*Fin
*Face Det
*Record Based Verification
Results:
Persons present in the scene:
Number of faces detected:
Sampling Face
Securing Databases of Higher Educatinal Institutions
Search the web and Windows
4:29 PM
3/13/2019

No Matching face

No Matching face. Please maintain a proper focus on camera

Fig. 4.11 Face Recognition Picture box

Output Design:


home
FaceCheck
Multilevel
Protect Your Tech
Biometric Verification System
Login here
Verified
*Fingerprint Verification
*Face Detection and Recognition
*Record Based Verification
Clear fingerprint
Cancel
Recocognize Face
Securing Databases of Higher Educatinal Institutions
Search the web and Windows
4:32 PM
3/13/2019

Results:

Persons present in the scene:

Babatunde,

Number of faces detected:

1

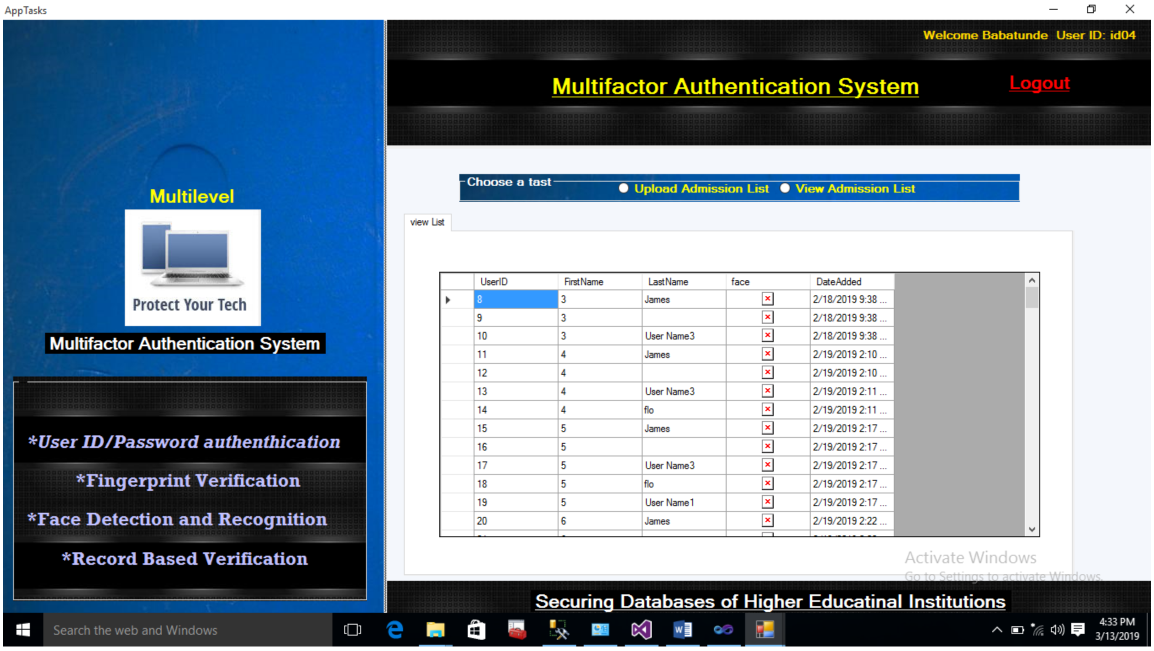
Click to Continue

* Matching faceDetected for Babatunde * Access granted. * Click Countinue

Verified.

Note:

Fig.4.12 Face detection Picture Box


AppTasks
Welcome Babatunde User ID: id04
Multifactor Authentication System
Logout
Multilevel
Protect Your Tech
Multifactor Authentication System
*User ID/Password authenthication
*Fingerprint Verification
*Face Detection and Recognition
*Record Based Verification
Securing Databases of Higher Educatinal Institutions
Search the web and Windows
4:33 PM
3/13/2019

Choose a tast ○ Upload Admission List ○ View Admission List

view List

	UserID	FirstName	LastName	face	DateAdded
▸	8	3	James	☒	2/18/2019 9:38 ...
	9	3		☒	2/18/2019 9:38 ...
	10	3	User Name3	☒	2/18/2019 9:38 ...
	11	4	James	☒	2/19/2019 2:10 ...
	12	4		☒	2/19/2019 2:10 ...
	13	4	User Name3	☒	2/19/2019 2:11 ...
	14	4	flo	☒	2/19/2019 2:11 ...
	15	5	James	☒	2/19/2019 2:17 ...
	16	5		☒	2/19/2019 2:17 ...
	17	5	User Name3	☒	2/19/2019 2:17 ...
	18	5	flo	☒	2/19/2019 2:17 ...
	19	5	User Name1	☒	2/19/2019 2:17 ...
	20	6	James	☒	2/19/2019 2:22 ...

Fig.4.13 Database Back End

VI. CONCLUSIONS

Conclusively, since it is an established facts that information remains the mainstay of any organization and confidentiality, integrity and availability are the hallmarks of database security, then security of organizations' databases is of paramount importance. It is however very crucial to device a strong security measure to safeguard database against unauthorized access. Securing database using multi-factor authentication will be the best solution to this, as combination of username, password and biometric systems give strong authentication to database. The combination of who you are, what you know and what you have. This dissertation studied the financial and technical features of Securing database using multi-factor authentication. There exist some flaws in data security of the old system which leads to serious problems, several issues of concern need to be proactively attended to, the security measure through the use of Personal Identification Number needs to be addressed with an alternative strong authentication measure.

VII. RECOMMENDATIONS FOR FURTHER STUDIES

Sometimes it is incorrectly assumed that doing nothing will cost an organization nothing. In reality, doing nothing related to the database security strategies discussed in this dissertation can cost an organization millions. Organizations need to consider database security as a part of their overall security strategy. Security is everyone’s responsibility, this means the DBA must play a role, as well as the security department and end users with access. Management should clearly define the roles of DBAs, security departments, auditors and others within the institution to ensure that database security risks have been addressed and that proper separation of duties is maintained when new controls are implemented. By providing an overall strategy for the environment, management can encourage different departments to work together to meet the organization’s overall security requirements. The good news, today, is that organizations are becoming more aware of their database security issues. Now they need to wrap robust database security strategies into their overall security and compliance strategies. Moreover, database vendors should add some excellent security enhancements that can greatly reduce the overall risk the database faces within a given environment. Such advancements will help organizations put security close to their critical data and better meet regulatory requirements.

- It is recommended that organizations including schools should employ MFA system to help reduce the level of impersonation/frauds as biometric traits will be required to gain access into the database.
- It is also recommended for the security of data and information, which is the major challenge and issue facing almost all institutions.
- This should be recommended for security organizations such as Security agencies like SSS, Police, CTU etc. so as to checkmate frauds at all levels and for criminal and civil investigations.
- It is also recommended for companies and industries to help improve the rate of information security in their companies.
- It is as well recommended to corporate bodies in other to secure their data and information since it can be encrypted using biometric technology which has physiological characteristics.
- Higher educational institutions should introduce it to every facet of their information systems etc.

Moreover, Subsequent researchers can combine other biometric features like Iris Scan, Retina Scan etc. with traditional username and password.

REFERENCES

[1] K. Beaudin, College and university data breaches: Regulating higher education cyber-security under state and federal law, August, 2015. Journal of College and University Law, *41* (3),pp. 657 - 694.

[2] E. Chabrow, China blamed for Penn State breach - Hackers remained undetected for more than two years from databreachtoday.com: 2015

[3] Grama & Joanna, Just in time research; Data breaches in higher education. EDUCAUSE. https://net.educause.edu/ir/library/pdf/ECP1402.pdf. October, 2015.

[4] A. Jain, L. Hong, & S. Pankanti, Biometric identification in Communication San Francisco: John Wesley Publishers, 2000.

[5] Grama, Joanna, et. al. (2016). Just in time research; Data breaches in higher education. EDUCAUSE. https://net.educause.edu/ir/library/pdf/ECP1402.pdf

[6] A. Greenberg, 2014,. North Dakota University System hacked, roughly 300K impacted. from SCmagazine.com: http://www.scmagazine.com/north-dakota.

[7] T. Danny, 2017 MFA (Multi-Factor Authentication) with Biometrics. 2017. Available online: https://www.bayometric.com/mfa-multi-factor-authentication biometrics/ (accessed on September, 2018).

[8] A.K. Jain (2005) Biometric Recognition: How Do I Know Who You Are? USA, Springer publishers.

[9] D. W. Davics & W. L. Prince. Security for Computer Networks. London: History Magazine

[10] V.A Duwy (2007) Digital Human Modeling London, Jenevik publishers Efliong

[11] https://punchng.com/african-universities-battle-hacking-cyber-crimes/. Accessed on 18th November, 2018.

[12] http://www.emgu.com/wiki/index.php/Main_Page Accessed on 13th Aprl, 2019.

[13] https://globalnews.ca/news/5412780/desjardins-user-data-shared/ Accessed on on 27th June, 2019.

[14] Emgu CV 2017 *Architecture Overview* (Online) available at http://www.emgu.com/wiki/index.php/Main_Page #Architecture Overview (on access dated August 19, 2018)

[15] J. Mc-Cune, Perrig M.& M.K Reiter. ”Seein-is-Believing: Using Camera Phones for Human Verifiable Authentication”, November 2004.

[16] Svitek, P., & Anderson, N. (2014). University of Maryland computer security Breach exposes 300,000 records. From WashingtonPost.com: http://www.washingtonpost.com/local/college-park-shady-grove-campuses-affected.

[17] The Australian Cyber Security Centre (ACSC) available at http://www. acsc.gov.au

[18] https://www.emgucv.com