Multi Factor Authentication for Student and Staff Access Control

Consuela Simukali[1]
School of Engineering, Department of Electrical and Electronic Engineering, University of Zambia, Lusaka

Jackson Phiri[2]
School of Natural Sciences, Department of Computer Science, University of Zambia, Lusaka, Zambia

Stephen Namukolo[3]
School of Engineering, Department of Electrical and Electronic Engineering, University of Zambia, Lusaka, Zambia1

***Abstract*—This paper proposes a model to improve security, by controlling who accesses the University of Zambia Campus, Student Hostels and Offices. The proposed model combines Barcode, RFID, and Biometrics Technology to automatically identify Students and Staff. A component to track visitors' physical location and movements in real time is also included to ensure visitors go to authorized places. A baseline study based on International Standard Organisation 27002 standard was conducted to measure the level of security at UNZA. This result shows that UNZA has uncontrolled access into the campus environment, student hostels and offices. The results from this study were used to develop the proposed model. When the RFID reader installed at any of the entrances detects an RFID tag number, the system requests for a fingerprint scan and scans the database for a match. If both RFID card and fingerprint belong to a registered Student or Staff, the entrance door or Turnstile is released open and access is granted otherwise access is denied. In case of the visitor the National ID number is tied to the RFID tag number. The visitors' RFID tag has a GPS module fixed to it. Once the visitor is granted access their movements and physical location are tracked in real time.**

Keywords*—Security and access control; authentication; RFID; ISO 27002; barcode technologies

I. Introduction

As students and staff own more valuable property on campus theft becomes more common and sophisticated. More valuables are stolen leaving a bad effect on the students and staff [1] [2]. Access control and physical security are therefore essential to curb such thefts. Physical security is one of the most important and basic form of protection. It involves the use of physical controls for protecting premises, sites, facilities, buildings or other physical assets belonging to the critical areas. Physical security is the process of using layers of physical protective measures to prevent unauthorized access or harm. This harm can involve terrorism, theft, destruction, sabotage, vandalism, espionage and so on [3]. In view of Information Technology, physical security is about controlling access to facilities by restricting entry to a property, a building or room only to authourised persons. Identified entrances to areas or facilities have perimeter boundaries and need different access rules or levels of security [4]. Several access control systems have been implemented by researchers. Radio Frequency Identification (RFID) in conjunction with biometric technologies has successfully been used for security issues and identification of people. Areas where RFID has been used include bus and train station, airports, malls, movie theatres and so on [5]. For public institutions considerations in expense of the proposed security systems are undoubtedly important. RFID systems are relatively low cost and can transmit data without usage of guided media at reasonably efficient levels of security [6]. The University of Zambia is a public and biggest higher institution of learning in Zambia with 16,500 full time students, 5,000 distance students and about 1,400 staff of which 900 are academic staff. Of the 16,500 students 3,000 of them are accommodated on campus. This study focuses on improving security at the University of Zambia (UNZA). In our proposed system a solenoid operated Turnstile is operated via RFID Reader that initiates user identification and authentication. The systems also keep an audit trail of date, time in and time out of all system users. Authourised users that is Students and Staff information is pre collected from already existing UNZA database.

II. Literature Review

Several research works has been developed and implemented in access control and identification system based different technologies. Each technology comes with its own advantages and disadvantages.

III. Related Work

A. Biometric based Security and Access Control Systems

Biometric recognition is the use of individual biometric characteristics, such as fingerprint, face, and signature for automatically computerized recognition systems. Fingerprints are the most widely used and successfully implemented form of biometric recognition system successfully. Fingerprint is a reliable biometric feature which has a range of applications such as access control, classroom attendance, financial transactions and so on. Authentication is achieved based on person specific verification [8] . However, fingerprint images are rarely of perfect quality. They may be degraded and corrupted due to variations in skin and impression conditions [7]. Access control systems using the latest biometric technologies can offer a higher level of security than conventional password-based systems. Their widespread deployments, however, can severely undermine individuals' rights of privacy. Biometric signals are immutable and can be exploited to associate individuals' identities to sensitive personal records across disparate databases [9]. In [10] Radio

frequency identification (RFID) technology has been combined with face recognition based on neural network. The systems recognises the person holding the card to allow access. This ensures that the person allowed access is the authorised one and denies access if they do not match. A Radial Basis Function Neural Network (RBFNN) is used to learn the face of authorized card holders and save the parameters of RBFNN only. In [11] An Access Control Vehicle System based on camera installed at the parking entry. Firstly, the non-adaptive method is used to detect the moving object. An algorithm is used to detect, recognize and verify the face of the driver who want to enter to the parking. Viola-Jones method is used for face detection while LDA algorithm is used for face recognition.

B. Barcode based Security and Access Control Systems

Barcode is a visual representation of information in the form of bars and spaces on a surface. These bars and spaces are designed with different widths and consist of numbers, characters and symbols. There are different combinations of alphanumeric characters that are used in the representation of this information. Barcodes come in various types today examples include Code 128, Code 39, EAN and so on. Barcode Identification is one of the more trending automatic identification technologies. Applications of barcodes have been commonly used in shopping, Species identification, libraries and so on [12]. In [13] a student authentication and verification systems is developed using Barcode Scanner. This system is aimed at reducing manual work and also eliminating the use of multiple cards. The student is allowed access to the college facilities such as library and central computer center more easily but also only by use of authorised ID cards. In [14] a barcode recognition system is developed by using image processing. The barcode on the object to be identified is captured as an image instead of using a barcode scanner, this provides the convenience of observing data from the barcode with lower cost and can be done from anywhere any time. Barcoding systems are recommended as best practice for specimen labeling and point-of-care test barcoding because of the high overall strength of evidence of effectiveness. In [15] studies demonstrate that barcoding reduces identification errors and improve accuracy of patient specimen and laboratory testing identification in hospital settings.

C. RFID based Security and Access Control Systems

Radio Frequency Identification (RFID) technology utilizes the electromagnetic fields for data transfer in order to perform automatic detection and tracking of tags or tags of objects. It can provide ways to design and implement relatively inexpensive systems particularly for security aspects. Many organisations use security personnel to control access to secure places but this is not sufficient considering the security challenges being encountered today. Electronic access control systems can be used as an additional layer of security. RFID based security system is one of such applications. In [16] an RFID based access control system with GSM is installed at the entrance of a secured environment to prevent an unauthorized individual access. A security and access control based on RFID and biometrics is proposed for use in University Hostels to differentiate between valid and invalid users. This system accomplishes the security and access control task by processing information from sub-controllers which include entrance monitoring controller, exit this tag number in non-volatile RAM. When the RFID reader installed at the entrance of hostel detects a number, the system captures the user image and scans the database for a match. If both the card and captured image belong to a registered user, access is granted; otherwise the system turns on the alarm and makes an emergency call to the security van through GSM modem [17]. A digital access control system has been installed to a protected area where none but people with authenticated credentials can enter. In [18] the implemented system comprises of digital door lock which is unlockable in real time to ensure secured access specifying activation, authentication and validation of users prior to bringing the RFID card close to the reader. The entire system is connected to central client-server sub-system that ensures and maintains the overall system.

IV. METHODOLOGY

A. Baseline Study

A mixed method approach was used in this study; qualitative and quantitative. For quantitative data, three questionnaires were designed based on ISO 27002 standard with focus on Physical Security and Environment best practice and guidelines. Questionnaires were distributed to 150 students, 120 members of staff (Academicians and Support Staff) and 10 Security personnel. The study focused on the Physical Security and Environmental controls of the ISO 27002. Fig.1 shows the different ISO 27002 Controls among which Physical Security and Environment control is. The following are the best practice and guidelines from the Physical and Environmental control:

1) Secure areas should have measures implemented that prevent unauthorized physical access, damage or interference to the organization's premises and infrastructure by using controls that are appropriate to the identified risks and the value of the assets to be protected.

2) Physical security perimeter should be used to protect areas that contain information and assets important to the organisation such as the people. Entry into the physical perimeter should be controlled by use of walls, controlled entry doors/gates, manned reception desks and other measures. Additional physical barriers where appropriate to prevent unauthorised access and physical contamination should also be used. The measures put in place should be designed in such a way that sufficient redundancy such as single point of failure are taken care of to ensure security is not compromised. Use of appropriate intrusion detection such as video and surveillance can enhance physical security. The walls should be built of an appropriate strength, the windows protected with bars while the doors should be protected with grill gates.

3) Physical entry control should be controlled in such a way that appropriate entry controls are implemented to ensure that only authorized personnel are allowed access. Appropriate controls would include such as authentication mechanisms, recording of date/time of entry and exit, and/or video

recording of activities in the entry/exit area. Appropriate identification used should be visible. Authorization and monitoring procedures and regular review of all these implemented mechanisms should be done. Authentication mechanisms examples include a keycard or PIN. It should be a requirement for authorised persons to wear visible identification and if any are not abiding they should be reported. Access rights should also be denied were appropriate.

4) Secure offices, rooms and facilities should have their own appropriate physical security designed and implemented commensurate with the identified risks and value of the assets in each setting. Secure offices, rooms and facilities should where appropriate should have unobtrusive or hidden controls and facilities especially for highly sensitive assets. Information about the location of sensitive facilities should be very restrictive. Measures that balance relevant health, safety and related regulations and standards should also appropriately be implemented. The figure below shows the ISO 27002 format and structure [19].

B. Current Business Process

Onsite visits and observation of the current business process were done. Every paid up and accommodated student receives a steel key to access the hostel room. Members of Staff are also given a steel key to allow entry into the office

1) Student scenario: When a student arrives at the campus, they go through the perimeter gate without any form of identification. To go to a students' room a student goes through the hostels' perimeter gate without any need to show identification. The students also enter through the Hostel building entrance without any form of security check and then finally enter their room by unlocking the door with a steel key. Fig. 2 shows the current student access level into campus.

2) Staff scenario: We take a staff who is a motorist. They drive through the university gate without the need to show identification. Random requests for identification by security guards are done but on an irregular basis. The Staff goes through main office building without identification and into his office where access is controlled by a steel key. Fig. 3 shows the current student access level into campus.

A.5Security Policy			
A.6Organisation of Information Security			
A.7 Asset Management			
A.8 Human Resource Security	**A.9 Physical Security and Environment**	**A.10 Communications & Operations Management**	**A.12 Info. Systems Acquisition development & maintenance**
A.11 Access Control			
A.13 Information Security Incident Management			
A.14 Business Continuity Management			
A.15 Compliance			

Fig 1. ISO 27002 Security Control Model.

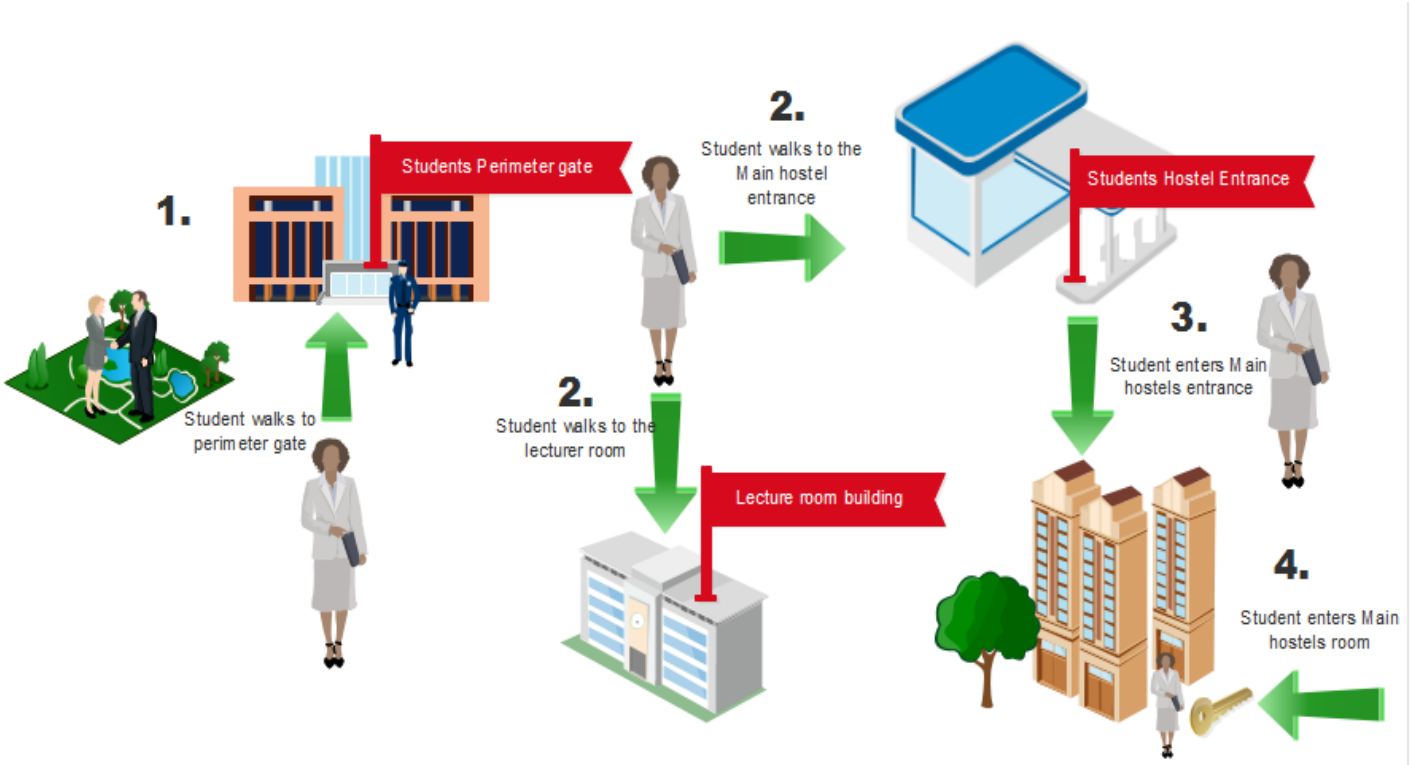

Fig 2. Current Business Process of Student Access into UNZA.

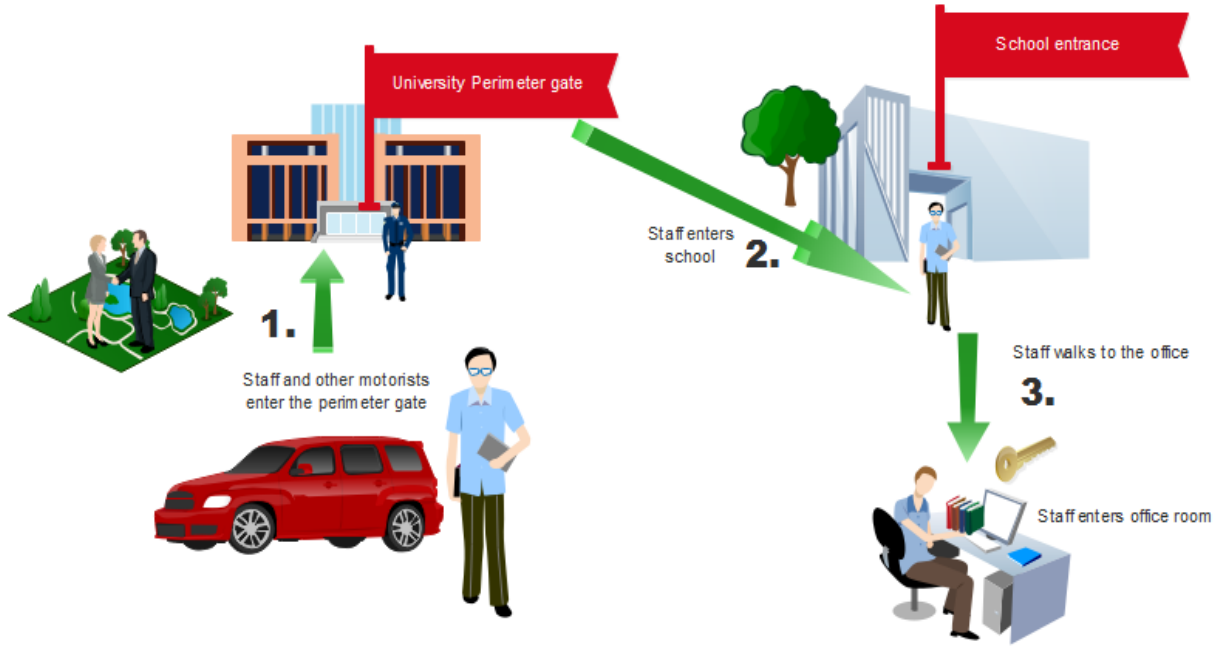

Fig 3. Current Business Process of Staff access into UNZA.

3) Barcode based identification: In the current business process every student registered or staff employed is given an ID card with a barcode printed on. The barcode is tied to the person's credentials such as Employee Number or Student ID

C. Proposed Model

The results of the base line study were used to design a model from the current business process. Fig. 4 below shows the proposed design of the model.

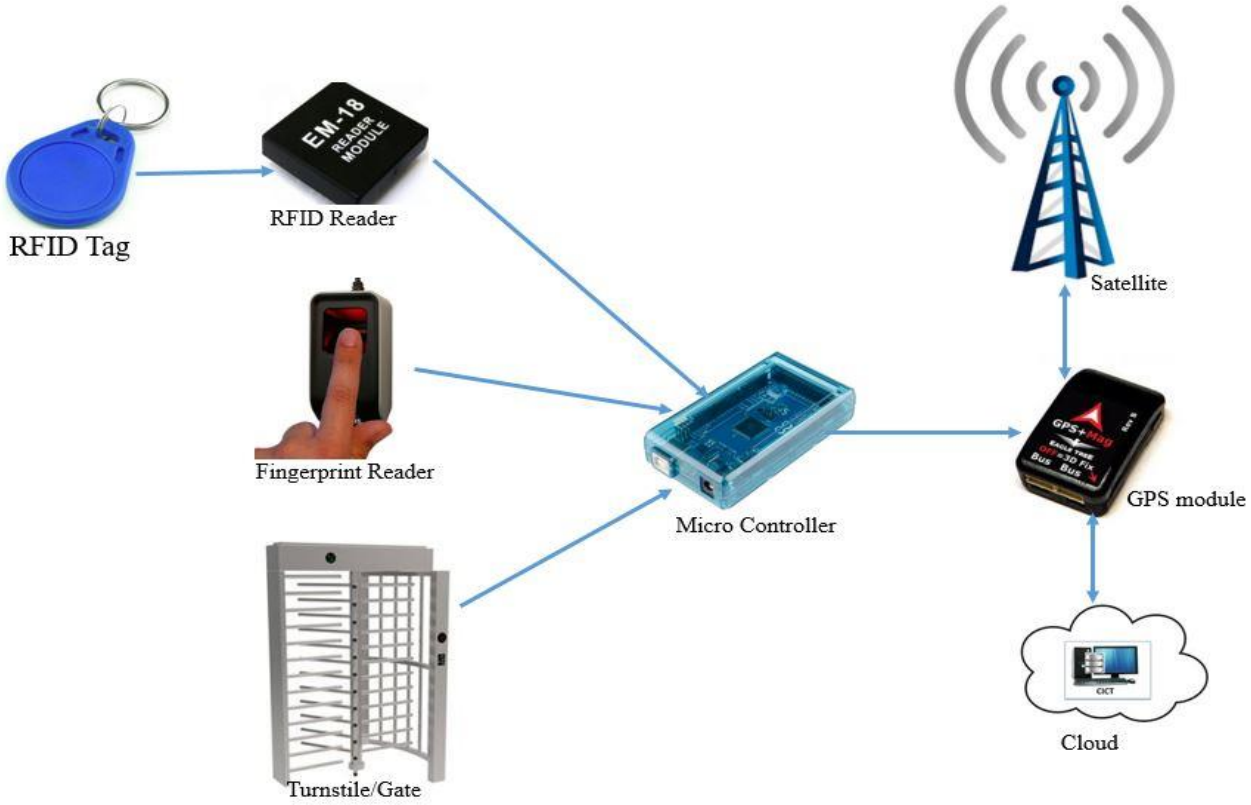

Fig 4. Proposed Access Control Business Model.

In the proposed model an RFID reader and Fingerprint scanner are fixed onto a Turnstile or Door of the entrances into the campus or facility such as room or office. The RFID reader and Fingerprint scanner are connected to the serial ports of the microcontroller. The data received by the reader and scanner are validated by microcontroller and sends the RFID and location through the wireless network to Database Server. The Application program in the Server validates the RFID User's location stored with the database. The Visitors RFID has a GPs receiver module attached to it. The modules send information to the cloud about their real time physical location while on campus.

D. Student and Staff Access

- Step 1: A user such as Student of Staff who wishes to have access to the campus physical environment, student hostel, office or any facility will foremost place their finger on the Fingerprint scanner (Fingerprint module). If the finger matches with the finger image in the database, then it goes to step two. Otherwise an error message is displayed requesting for a valid finger. If this attempt fail for the third time the systems goes to the initial condition which is; place a valid fingerprint.
- Step 2: In this step the user is required to place the RFID card against the RFID reader. If it is not a valid identification as in step one, the system will display a message requesting the User to place a valid RFID card. If the identification of the RFID card is valid the Door or turnstile will be opened allowing access into the facility.

E. Visitors' Access

Any Visitor to the university will be required to show an identity such as National Registration Card or Drivers' license. The number of the identity is matched to an RFID's unique code. The visitors are required to have this card wherever they go on Campus in order to have entry.

F. Barcode based Identification Transformation to RFID based

The study proposes an algorithm that uses already existing student and staff credentials tied to the barcode to be transformed to RFID based identification. During registration stage the student or staff captured fingerprint is tied to the RFID Unique Identification Code (UIC). The UIC is then tied to the already existing Barcode.

V. Findings

A. Results from Baseline Study

A baseline study was conducted to measure the level of security at the University of Zambia. A questionnaire based on ISO 27002 standard guideline or physical and environmental security was designed to measure this level of security. The results show that UNZA's level of security needs improvement due to several factors. The survey reviews that the most commonly stolen property from students and staff is media such as laptops and mobile phones [20].

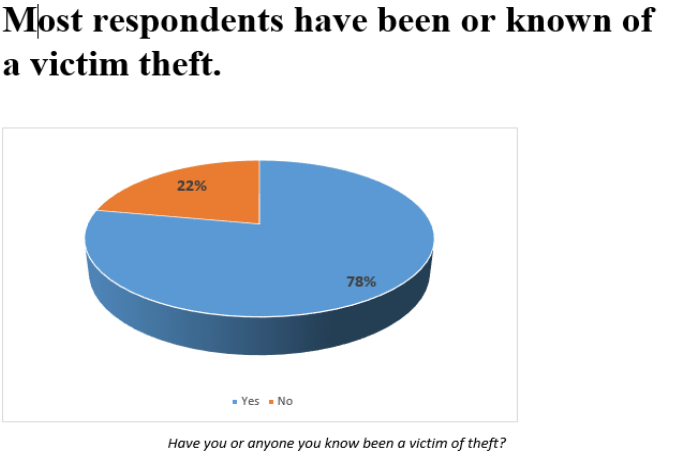

Fig 5. Victims of Theft.

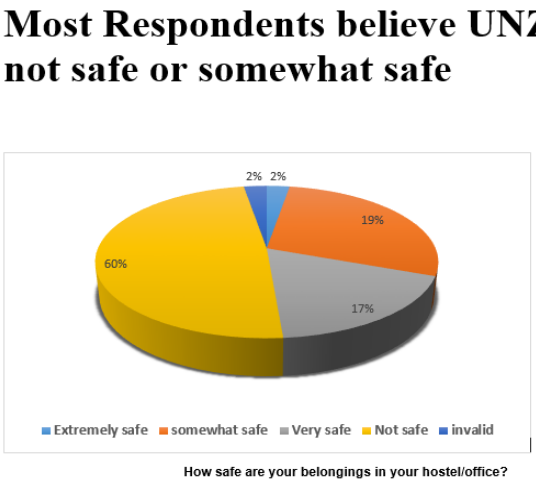

Fig 6. UNZA's Level of Security.

When asked whether any student or staff has been a victim of theft on Campus. The results showed that more than 78% of the respondents have been a victim or known of a victim of theft on campus. While less than 22% have never been victims or known of one as shown in Fig. 5.

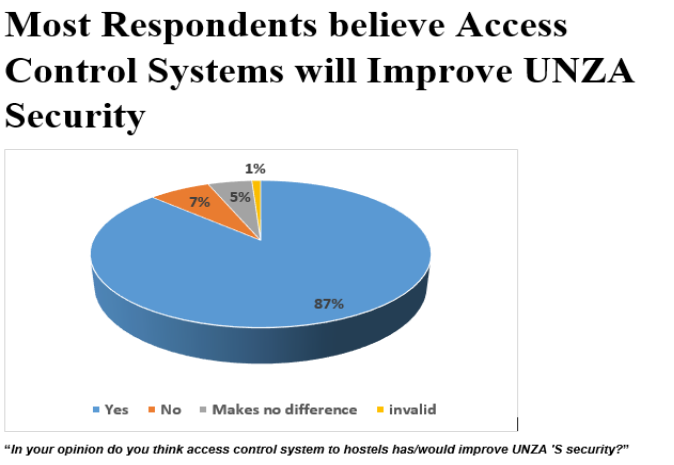

Fig 7. Access Control System Opinion.

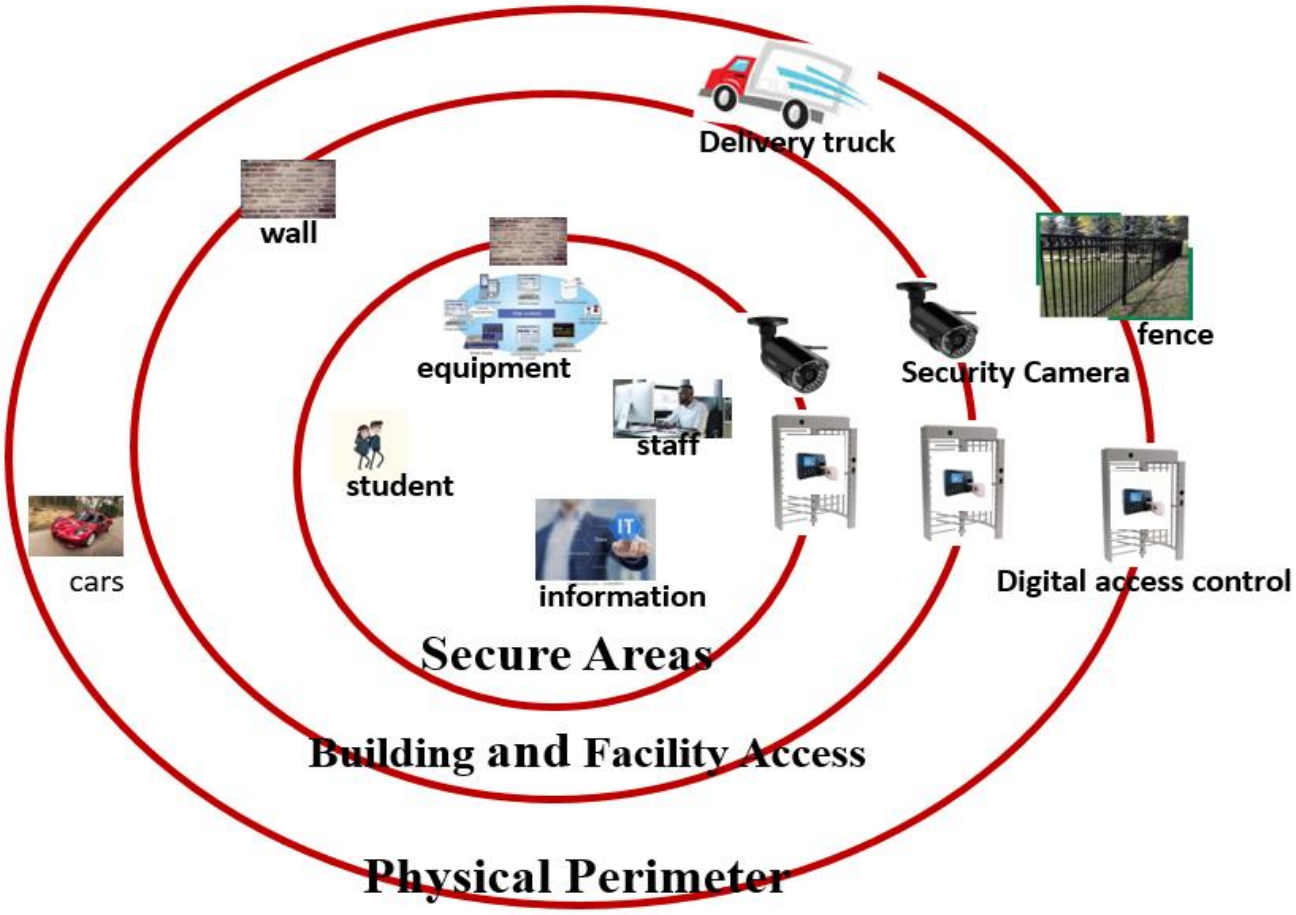

Fig 8. Layered Security Model.

Fig. 6 reveals results from both students and staff's view of safety of UNZA. The study reveals that out of the 120 students and 100 staff who filled in the questionnaire, only about 2 % believe UNZA is extremely safe, about 17% believe UNZA is very safe, 19% believe UNZA is somewhat safe while more than 60% believe UNZA is not safe.

In Fig. 7 the study reveals that 87% respondents believe access control systems can improve security at UNZA, 7% respondents do not believe access control systems can improve security at UNZA while 5% respondents believe access control systems will not make a difference.

B. Layered Approach Physical Security

The Student and Staff Access Control is based on the ISO 27002 Physical and Environmental Security This model gives more of a mix approach between restrictive and permissive approach. Once people are allowed into an area they can go anywhere within that area though movements between areas is more restrictive.

"Fig. 8 illustrates the proposed model for UNZA. Moving from one area such as Physical Perimeter to Building and facility area is defined by procedures for moving from one level to another. As people transition from the outside to the inner most secure areas, it should be extremely difficult to move between unauthorised ways. As students, staff or visitors move from one area to another they have to use provided identification and authentication systems provided. Records such as date, time and door or gate accessed will be recorded.

In the proposed model Secure areas, Physical perimeter and secure building and facilities are protected with wall and fence of appropriate strength. Audio and video surveillance and automated identification and authentication mechanism are also implemented to ensure access into the facilities is allowed only to authorised persons".

VI. Discussions and Conclusion

Analysis of our survey data identifies key points in the level of security and access control at the University. It strongly shows that security is porous and not all entrances in perimeter or facilities have access control systems implemented. Anyone can easily enter the campus and there is no way of identifying who is a visitor or who is authorised to have access to offices or student hostels.

We have introduced a multifactor authentication system based on RFID and Biometrics to allow the University of Zambia to allow access to the campus only to authorised people. To address the challenge differentiating an ordinary

visitor or contractor from student or staff, we introduced a visitor identification and monitoring module.

Integrating the biometric system into the RFID based access control systems ensures that the real owner of the RFID tag is authenticated and allowed access so than a user can use a Tag that does not belong to them but is still allowed access.

ACKNOWLEDGMENT

We would like to acknowledge the Students, Staff and Security Personnel for their valued responses to the baseline study questionnaires.

REFERENCES

[1] Z. K. Zhu Yuan-jiao, "Design and Realising of the Digital Campus Security system,," in *WRI World Congress on IEEE*, 2009.

[2] T. S. J. Z. C. S. Xi Li, "A Sptil Technology Approach to Campus Security," in *Networking, Sensing and Control, ICNSC IEEE International Conference on IEEE*, 2008.

[3] V. V. Annarita Drago, " Methods and Techniques for Enhancing Physical Security of Critical Infrastructures Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione," March 2015.

[4] F. T. S. F. a. B. O. W.M. Fitzgerald, "" Anomaly analysis for Physical Access Control security configuration,"," in *7th Int. Conf. Risks Secur internet Syst.*, 2012.

[5] G. T. P. K.Srinivasa Ravi, " RFID Based Security System," *International Journal of Innovative Technologyand Exploring Engineering(IJITEE)*, Vols. Volume-2, 3, no. Issue-5, , pp. ISSN: 2278-3075,, April 2013.

[6] G. v. a. P. Tripathi, " A Digital Security System with Door Lock System using RFID Technology," *International Journal of Computer Applications*, vol. Volume 5 August 2010, no. No. 1 1, p. (0975 – 8887) , August 2010.

[7] A. V. P. A. K. M. K. M. Yash Mittal, "“Fingerprint biometric based Access Control and Classroom Attendance Management System”," *Annual IEEE India Conference (INDICON)*, 2015.

[8] A. El-Sisi, " Design and Implementation Biometric Access Control System Using Fingerprint for Restricted Area Based on Gabor Filter," *International Arab Journal of Information Technology*, pp. 8(4):355-363, October 2011.

[9] Y. L. J. Z. ,. S.-C. C. Shuiming Ye, " “Anonymous Biometric Access Control”," *EURASIP Journal on Information Security*, vol. 865259, 2009.

[10] W. W. Y. N. P. P. K. C. H. D. B. J. a. D. S. Y. D. Wu, " "Access control by RFID and face recognition based on neural network,"," International Conference on Machine Learning and Cybernetics,, pp. pp. 675-680., 2010.

[11] Taleb, M. E. Amine Ouis and M. O. Mammar, "Access control using automated face recognition: Based on the PCA & LDA algorithms," *2014 4th International Symposium ISKO-Maghreb: Concepts and Tools for knowledge Management (ISKO-Maghreb)*, Algiers, 2014, pp. 1-5.

[12] S. &. H. M. &. A. A. A. &. A. A. I. Yakub, Attendance Management System Using Barcode Identification on Students' Identity Cards. , (2016).

[13] A. K. P. J. A. G. L. M. S. V. G. Akshatha M., "“Student Authentication and Verification System using Barcode Scanner”," International Journal of Internet of Things, vol. 6(2):, pp. 71-74, 2017, .

[14] N. A. I. N. M. S. F. S. Z. Z. ,. N. M. Z. Hashim, " “Barcode Recognition System”,," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, Vols. Volume 2, , no. Issue 4, , July – August 2013.

[15] S. R. e. a. Snyder, " “ pp. 13-14 , 2012

[16] J. M. M. G. A. I. Peter Adole, " RFID Based Security Access Control System with GSM Technology ,"," *Journal of Engineering Research (AJER)*, , vol. 5, no. 7,, pp. pp 236-242.

[17] M. u. H. M. A. A. H. M. U. A. Umar Farooq, "“RFID Based Security and Access Control System.”," *IACSIT International Journal of Engineering and Technology*, , Vols. Vol. 6,, no. No. 4,, August 2014.

[18] M. Kishwar Shafin et al., " "Development of an RFID based access control system in the context of Bangladesh,," *International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*,, vol. , pp. pp. 1-5., 2015.

[19] ”Code of Practice for Information Security Controls ,” Available: http://www.iso27001security.com/html/27002. [Accesed October 2018]

[20] UNZA, "UNZA Security Department," July 2018.