ISSN:2320-0790

An International Journal of Advanced Computer Technology

ARMOURY USER IDENTIFICATION AND CRIME DETECTION SYSTEM IN THE 151 BASE SERVICES GROUP (151 BSG) NAF BASE MAKURDI

Moses Adah Agana[1] and Akpan Idorenyin Beranard[2]

[1]Department of Computer Science, University of Calabar
ganamos999@yahoo.com
[2]Nigeria Air Force (NAF) Base Makurdi
mercy4eee2004@yahoo.com

Abstract: This study utilized biometric fingerprint recognition and Global system for Mobile Communication (GSM) Short Message Service (SMS) to identify military armoury users and alert possible intrusion to take arms without authorization respectively. This is aimed at holding accountable those assigned arms from the armoury to avert the diversion of arms for criminal tendencies. The existing armoury security system was critically evaluated through physical examination of the armoury in the Nigeria Air Force (NAF) Base Markudi and oral interview to elicit facts from custodians of the armoury. It was observed that armoury control records were kept manually and this is prone to non-accountability and arms smuggling to commit crimes in the society. The new system was designed using object oriented programming and implemented using Personal Homepage Pre-processor (PHP) and java, with MySQL as the database system. A fingerprint sensor was integrated with the system for biometric image capturing of users and the entire system is linked to a mobile telecommunication system for SMS alerts of possible intrusions. The new system can authenticate pre-registered users via fingerprint recognition before granting them access to the armoury strong room, with an SMS to the administrator. An authentication failure triggers an SMS of intrusion notice to the armoury administrator and also triggers surveillance security guards to arrest the intruder. The database keeps logs of all assigned arms with the users and intrusion logs for cross-referencing. The system is thus found useful in identifying armoury users and in detecting arms smuggling.

Keywords: Armoury, biometric, authentication, arms, security

I. Introduction

1.1 Armoury Usage and Misuse

An armoury (or arsenal) is a place for making, storing and maintaining arms and ammunition, training of personnel on arms usage, arms and ammunition allocation and the general administration of arms and ammunition [1]. Armouries are predominantly located in military formations in most nations, and because of the sensitive roles the military play in providing national and territorial security with the use of arms, the armoury should be well secured and properly managed [2].

Armoury usage covers issuance/receiving of arms and ammunition, weapons inspection/screening, maintenance, security control, storage, and weapon test-firing [3]. The armed forces of any nation is saddled with vital responsibilities of maintenance of peace, security of lives and properties of citizens, as well as the protection of its territorial integrity against all forms of external aggressions. The degree to which lives and properties are kept safe largely depends on the control of arms and ammunition and denial of accesses to unauthorized persons. Hence, lapses in security of these weapons could result in their possession by unauthorized and unscrupulous persons, which in turn poses an undesired threat to lives, properties and peace of the nation.

National security is of primary concern to the military and the role of human elements in security administration is prominent. However, over time, there has been increasing deficiencies in arms

management, especially in the armoury, causing arms smuggling and their misapplication to commit crimes in the society. These problems are largely due to the manual handling of armoury records that demands more human efforts, is inefficient and not adequately accountable. The adoption of cutting edge technologies to provide a more secure and efficient service thus becomes inevitable [4].

A predominant number of armouries are locked using padlock, password or smartcard based locks which can be easily compromised. Keys can be stolen or duplicated, passwords can be guessed or forgotten, and the Radio Frequency Identification (RFID) card can also be stolen or cloned [5].

Due to the use of traditional, insecure armoury management systems, there are reports of some soldiers being involved in stealing and selling arms to criminal gangs and even insurgent groups. One of such instances was cited in November 2007 by military and media sources that a syndicate had, over a long period, allegedly sold arms, including AK-47 assault rifles and general purpose machine guns, as well as ammunition, from the army's Central Ordnance Depot in Kaduna to some Niger Delta insurgents fighting the military [6][7]. The difficulty in stopping the Boko Haram insurgency in North Eastern Nigeria as well as the marauding activities of Fulani herdsmen in North central Nigeria and other parts of the country is not unconnected with this. There are also reports of a significant number of soldiers being involved in other criminal activities such as armed robbery, kidnapping, etc. as a result of arms smuggling [8][9].

In a related development, a burglary attack on 2 Division Nigerian Army Armoury was reported and investigations revealed that a criminal had secretly duplicated the armoury door key unknown to the armourer and used the duplicate key to secretly open and steal arms from the store while the sentries were off-watch [4]. Similarly, the armoury of the Nigerian Naval Base in Port Harcourt, NNS Okemini in was burgled in December 2015, where the password-based security door was easily opened by hoodlums without any physical damage to the door. Investigations after the rubbery revealed that the password was either guessed or leaked [4].

These scenarios are pointers to the fact that the use of keys, cards and passwords are not reliable to secure the armoury. To contend with such problems as those aforementioned, it is expedient to enforce design and management standards in armouries.

1.2 Armoury Protection

Besides the physical security provided by human sentries put in place, an armoury access door is usually placed under lock. Locks and keys have been in existence for centuries, but have undergone historic modifications ranging from mechanical to electronic, and from isolated to interconnected systems. For instance, some armouries use electronic time control that regulates the time of access for various users, often interfaced with turnstiles for entry control in buildings to prevent unauthorized access [5]. Without security personnel that are trained on the use and maintenance of physical security devices for armoury protection and who are able to properly respond to breaches in security, all the technological systems employed to enhance physical security of the armoury will not suffice. Security personnel perform many functions such as patrols, road checks at checkpoints, administration of electronic access control, response to alarms, monitoring and analyzing videos, etc.

The Unified Facilities Criteria (UFC 1-200-01) in the United States of America for instance specifies for all United States armouries at home and abroad, applicability of model building codes and government-unique criteria for typical design disciplines and building systems, as well as requirements for accessibility, antiterrorism, security, high performance and sustainability, and safety [10]. The requirements further specify the physical security measures of the armouries to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. The armoury management system controls inventory, storage, equipment repair and maintenance, delivery, management methodologies, and any additional functions accommodated in the specific facility. In addition, there should be a weapons distribution which protocol affects the layout of the facility. In most armories the weapons are distributed through issue ports that determine the types of weapons that can be issued and whose size is regulated by physical security requirements [10].

Advances in technology have produced a paradigm shift from traditional locks to programmable locks, with some making use of all kinds of authentication methods such as passwords, digital keys like security tokens, radio frequency identification (RFID) tags, automated short message service (SMS) alerts and of late biometric data like fingerprints [11][12]. Biometrics have been found to be the most reliable access control system in recent times because it is concerned with capturing, verifying and

authenticating unique physiological traits of users before granting access, based on the premise that no two persons can have the same traits of the biometric features captured. These new systems are not easily compromised like the traditional lock and security systems.

The use of biometric technique to implement a fingerprint lock system requires the use of a fingerprint scanner to detect the complex ridges of a user's fingerprint after capturing and storing in the database. The user's fingerprint in subsequent times is verified with the pre-stored one to authenticate that he is the rightful person before access is granted. Because fingerprint patterns are unique to everyone, any form of replication can be avoided; also, the fingerprint of a person does not change for his lifetime, which can ensure a long-term use. At the same time, there is no need for users to carry any form of physical objects because the users themselves are the keys. Moreover, with the addition of a mobile-based notification system, it is easy to alert security operatives of any intrusion. The limitations of fingerprint security systems are that high-quality sensors are needed to ensure the accuracy of the biometric data recognition and it may be expensive to implement. However, for security optimization and ease of accessibility, fingerprint enabled locks are presented as the optimal solution [13].

Biometric authentication in contemporary times is the most reliable security system ad as such will find useful application to compliment the physical security measures in preventing unauthorized access to the armoury to smuggle and misuse arms.

II. Related Works

Various security systems which enhance identification, verification and authentication have been proposed and implemented. These systems find applications in several domains such as law enforcement, industries, homes, schools, and banks, the military and other organizations.

A field programmable gate array (FPGA) – based personal authentication system using fingerprints and was designed and the proponents opined that the current technological age demands that the deployment of biometric security systems should not be restricted to stringent and highly reliable fields such as forensic, government, banking, etc. but should be extended to a wider range of daily use in consumer applications such as internet access, border control, health monitoring, mobile phones, laptops, etc. [14].

Also, an RFID based security and access control system for use in the Punjab University hostels premises has been designed. The system integrates RFID technology installed at the entrance with biometrics to authenticate and grant access to visitors and occupants of the hostel. When the RFID reader detects a number, the system captures the user's 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 triggers an alarm and makes an emergency call to the security van through a GSM modem, causing security operatives to respond and arrest the intruder [15].

In a related development, an electrocardiographic (ECG) application in multi-biometrics authentication was proposed by [16], postulating that the unique properties of ECG signals make them suitable for such an application to enhance security in hard biometrics systems and in standalone soft biometrics for low security and low user throughput applications. The designers maintained that the ECG system can be continuously measured, enabling a new class of applications to benefit from the continuous biometric perspective in user identification and authentication.

A microcontroller based authentication system for armoury security using RFID integrated GSM to authenticate users before granting them access to the armoury; thereby disallowing personnel without the valid RFID cards from gaining access to the armoury was designed by Ini-Mfon [4]. The system is however akin to the use of a physical metal key, which may not be convenient and could be stolen or lost. In addition, virus could possibly attack the RFID reader, thereby compromising the system.

In a related development, a mean-interval algorithm and personal mobile sensor card system for ECG verification was proposed for sportsmen, using biometric authentication. The proposed new mean-interval approach was designed to identify the user quickly with high accuracy, while consuming just a little amount of the microprocessor flash memory and does not necessarily require a centralized database. Their experimental results were tested on public MIT-BIH ECG databases using the designed circuit system and confirmed that the proposed scheme is able to provide excellent accuracy and low complexity [17].

III. Methodology

The object oriented methodology was adopted in the design of the armoury user identification and

smuggling detection system. The design was modeled far application in the management, collection and return of arms and ammunition from the 151 BSG armouries, Nigeria Air Force (NAF) Base, Makurdi. The design was implemented using java and Adobe Dreamweaver with MySQL as the database management system.

The existing system was critically reviewed based on its modus operandi and the gaps therein were used to model the new system. The existing security system of the NAF armoury is predominantly manual. The building has vault doors or solid hardwood with a steel plate on the outside face, and with door bucks, frames, and keepers rigidly anchored. The doors are secured with padlocks and hasps. Windows and other openings are kept to a minimum, closed and firmly locked. Armoury doors are kept locked or bolted from the inside when individuals are working inside.

Patrols are made at prescribed intervals, and random checks are also conducted. Some security staff are designated, trained and properly equipped, and are ready to react in a timely fashion to respond to possible incidents. Military working dogs are also used as a complementary measure. There is a perimeter fence with an entrance gate and a clear zone around it. The armoury keys are issued only to those personnel who require access in order to perform their official duties. The number of keys to the armoury is minimal and not easy to reproduce. An armourer is kept on duty to take inventory of arms signed out and arms returned as well as particulars of those assigned the arms. The armourer apparently has little idea about how many arms and ammunition are in stock in the armoury. Though sometimes the record exists, but the time taken to account for the arms signed out and those returned is too long for proper accountability. The armourer can also compromise issuance of arms to some authorized persons and is prone to arms smuggling without tracking the identity of the smugglers. It was also observed that the manual keeping of arms records gives room to missing of some arms and difficulty in tracking those who sign for arms without returning them.

The proposed system was modeled to contend with the problems identified in the existing system. The system was designed such that access to arms is based on biometric authentication of users (finger print capturing) in addition to the username and password. Only duly registered and authenticated users can be granted access to the armoury to collect arms, and a comprehensive record of arms and ammunition in stock and those issued/returned is kept in the database. In the event of any unauthorized user trying to access the armoury, an SMS alert is sent to the armourer, and also to security guards to arrest the intruder. The requirements of the proposed system include the data about NAF personnel concerned with access to the armoury, the types of weapons available and their specifications, the method of signing out and signing in of arms (weapons) and parameters involved in the process. In the new system, it is easy to track whoever signs for arms and ammunition without returning them. Figure 1 shows the schematic view of the proposed system as described above.

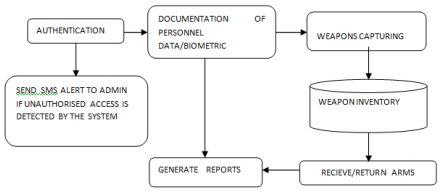

Figure 1: Schematic View of the Armoury User Identification and Crime Detection System

Figure 2 illustrates the system flowchart for arms allocation, specifying authentication and intrusion detection. A valid user should be registered before accessing the system, otherwise he is considered to be an intruder.

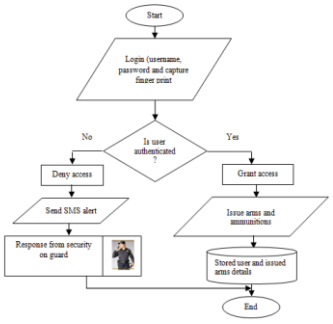

Figure 2: System flowchart for arms allocation

The arms return process equally follows the same process of authentication as illustrated in figure 3.

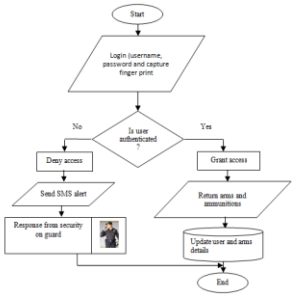

Figure 3: System flowchart for arms Return

The system design was implemented and tested using Enterprise Java Beans (EJB 3) and MySQL as the database management program, while Digital Persona Fingerprint Scanner was used as the plug in to capture and authenticate users' fingerprints. The system testing was done using live data at the NAF Base Makurdi armoury. Some Air Force personnel were used to validate the results of the system by registering, signing for arms and ammunition, and returning them.

IV. Results

The results obtained are presented and discussed in this section. The system utilizes a two-factor authentication to grant full access to a user to collect arms and ammunition from the armoury. The first level of authentication requires only the username and password of the person seeking to collect arms. The second level is the biometric authentication that captures and verifies the user's fingerprint. The login module is the first interface the system user encounters when the system is launched. It provides the user with two input fields to provide username and password. If the details provided correspond to what is stored in the database, the user is authenticated and is granted access to the system home page. Otherwise, the user is denied accessed and an intrusion alert is initiated via an SMS to the armourer and security guards. The login module is illustrated in figure 4.

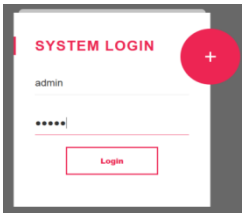

Figure 4: Login Module of the Armoury User Identification and Crime Detection System

Upon successful authentication of the user, using the registered username and password, the system loads the user's home page. The home page has menus linking actions that the user can perform and acts as a container for other actions that can be triggered by the user. But before any further action, the second tier of user-authentication must be performed. This is the biometric authentication by fingerprint capturing and verification. Figure 5 shows the home page.

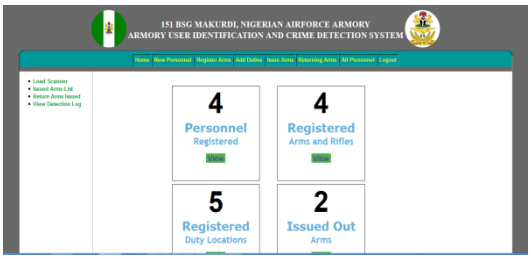

Figure 5: Home Page of the Armoury User Identification and Crime Detection System

A new user has to register from the home page before proceeding. The registration form is illustrated in figure 6. The personnel bio-data is stored together with the fingerprint for matching and verification anytime the personnel requests for arms and ammunition.

Figure 6: Personnel Data Capture Form

From the home page, the user has to load the scanner for fingerprint capturing and verification before proceeding further. A dialogue box indicating that the scanner has been loaded is illustrated in figure 7.

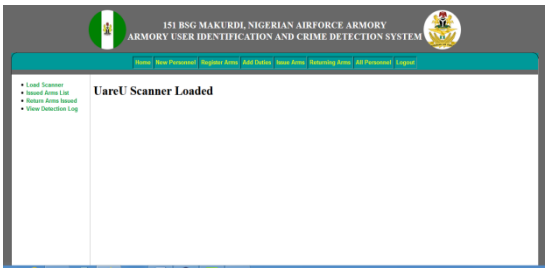

Figure 7: Fingerprint Scanner loaded

The successfully scanned fingerprint is shown in figure 8. This serves as an input for further verification and authentication before any arm or ammunition can be issued to the applicant.

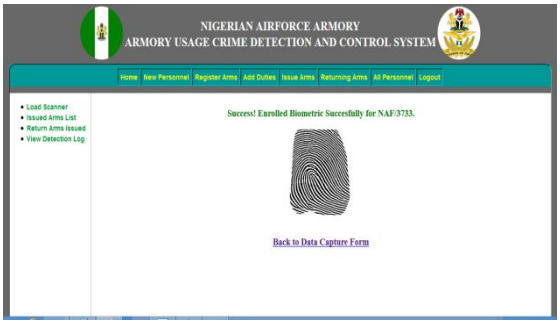

Figure 8: Enrolled Fingerprint for further Verification and Authentication

The fingerprint is verified with the user's previous records in the database, if it matches, the user is authenticated and can proceed to collect arms and ammunition. Figure 9 illustrates the records of a successfully verified and authenticated user.

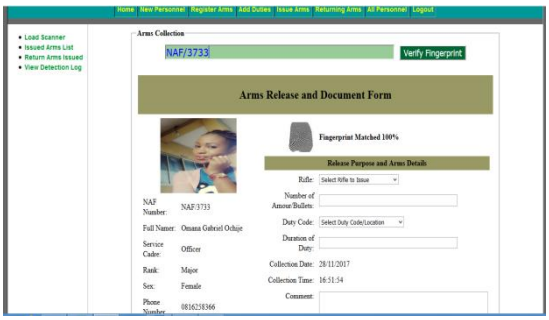

Figure 9: Successful Fingerprint Verification

If the fingerprint verification fails, an impersonation alert is triggered and an SMS message is sent to the armourer and the air intelligent wing for proper follow up. Impersonation log is also documented by the system which is accessible for further decision making. Figure 10 illustrates the impersonation alert.

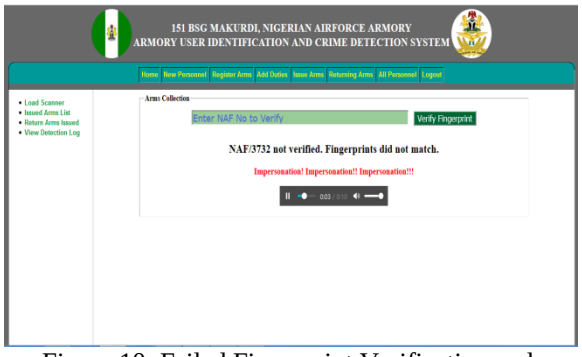

Figure 10: Failed Fingerprint Verification and Impersonation Alert

A record of all impersonation logs is maintained by the system for easy verification and appropriate actions as illustrated in figure 11.

Figure 11: Impersonation Detection Log

A database of all duly registered personnel who can be verified and authenticated any time they request for arms is maintained by the system as illustrated in figure 12.

Figure 12: Database of Registered Personnel

The equally maintains a database of all arms of ammunition for accountability. With this, it is easy to verify arms and ammunition issued out and returned. Missing arms can equally be traced to those who signed for them. Figure 13 shows the records of arms in the armoury.

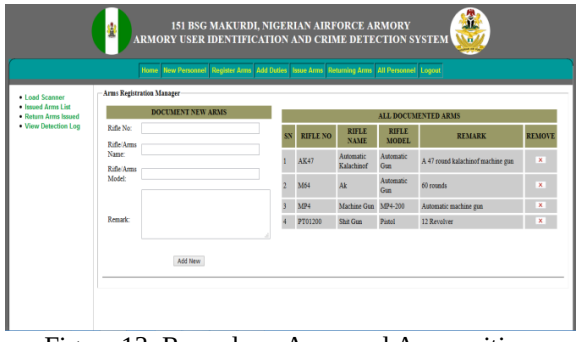

Figure 13: Records or Arms and Ammunition

The system also keeps records duty locations where the personnel assigned arms and ammunition have been posted for military operations. This is done so

that is easy to trace where assigned arms and ammunition are being taken to as well as to track missing arms and related armoury use crimes. The duty location records are illustrated in figure 14.

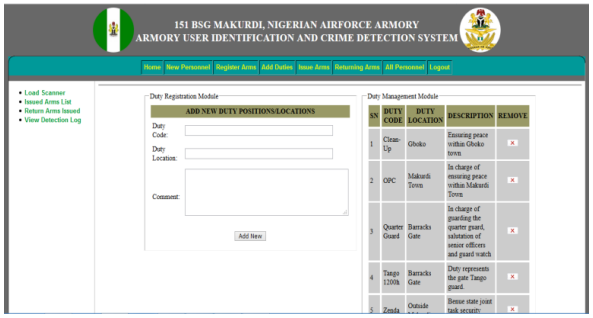

Figure 14: Duty Location Records

There is also a record of issued arms associated with the duty locations and the users for easy verification of return or misuse. This is illustrated in figure 15.

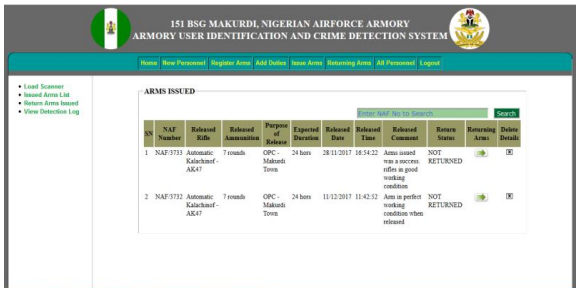

Figure 15: Issued Arms List

The record of all successfully returned arms and ammunition is maintained as illustrated in figure 16.

Figure 16: Record of Returned Arms

V. Conclusions

Implementing new technology is always a challenging though quite important for an organization. The decision on which technology should be implemented and how it will be implemented must be based on thorough analyses of how the technology will improve the process and what it will cost. This study has thus examined the traditional method of armoury inventory management and identified challenges faced by the existing method. This served as a pointer to the design of the new system that utilizes biometric authentication and a comprehensive database system to manage the issuance and return of arms and ammunition to the armoury. The new system equally provides SMS alerts to trigger quick security response to contend with any intrusion attempt into the armoury. The test results of the system in the NAF Base Makurdi proved efficacious. Its implementation will thus make amoury management more reliable, convenient, efficient, accurate and accountable.

VI. References

[1]. Owen L. Hewitt (2017). Armories. NAVFAC Engineering Criteria and Programs Office (CIENG). *https://www.wbdg.org/building-types/armories*. Retrieved 29-05-2018.

[2]. European Union (2004). Final Report on the Improved Weapons Record Keeping and Safe Storage

[3]. Project in Military Region 4, EU-Assistance on Curbing Small Arms and Light Weapons in Cambodia

[4]. Old, K. (2006). Armoury Building on Territory of the Russian Empire Nov 1917. Article 1256 of Book IV of the Civil Code of the Russian Federation No. 230-FZ. Ini-Mfon, U. (2016). Design and construction of Microcontroller Based Authentication system for Armoury Security. Masters of Technology (MTECH), Thesis, Obafemi Awolowo University, Ile-Ife.

[5]. Hayes, F. (2004). "RFID Doesn't Work - So Live With it!" http://www.techworld.com/mobility/features/index.cfm?featureid=872. Retrieved on 29-05-2018.

[6]. Sunday Punch (2008). "More startling revelations on missing military arms", Lagos, 20 January.

[7]. Nigerian Tribune (2008). , 15 January 2008. "How Nigerian army officers sold weapons to militants",

[8]. Daily Champion (2011). "How soldiers abducted Mikel Obi's dad – police", 24 August.

[9]. Vanguard (2015). "Police arrest soldier for supplying arms to robbers", 29 December.

[10]. Unified Facilities Criteria (UFC) (2014). Armories and Arms Rooms. U.S. Army Corps of Engineers: UFC 4-215-01, 1 December. http://www.wbdg.org/FFC/DOD/UFC/ufc_4_215_01_2014.pdf

[11]. Kamble, N.D. and Dharani, J. (2014). Implementation of Security System Using 3-Level Authentication. International Journal of Engineering Development and Research, 2 (2), 1528-1532. https://www.ijedr.org/papers/IJEDR1402039.pdf. Retrieved 30-05-2018.

[12]. Meera, M. and Divya, R.S. (2017). Super Secure Door Lock System for Critical Zones. Proceedings of the Networks & Advances in Computational Technologies (NetACT) International Conference, Thiruvanthapuram, India, 20-22 July. DOI: 10.1109/NETACT.2017.8076773

[13]. Azimpourkivi, M., Topkara, U. and Carbunar, B. (2017). A Secure Mobile Authentication Alternative to Biometrics . Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017), 7 December. https://arxiv.org/pdf/1712.02483.pdf. Retrieved 31-5-2017.

[14]. Fons, M., Fons, F., Canto, E. And Lopez, M. (2012). FPGA-based Personal Authentication Using Fingerprints. Journal of Signal Processing Systems, 66(2),153-189. DOI: 10.1007/s11265-011-0629-3.

[15]. Umar, F., Mahmood, H., Muhammad, A., Athar, H. and Muhammad, U. A. (2014). RFID Based Security and Access Control System. International Journal of Engineering and Technology, 6(4), 309-314. DOI: 10.7763/IJET.2014.V6.718.

[16]. Silva, H., Lourenço, A., Canento, F., Fred, A. and Raposo, N. (2013). ECG Biometrics: Principles and Applications. In Proceedings of the International Conference on Bio-inspired Systems and Signal Processing, pp. 215-220. DOI: 10.5220/0004243202150220.

[17]. Tseng, K., Zeng, F., Ip, W.H. and Wu, C. (2016). ECG Sensor Verification System with Mean-Interval

[18]. Algorithm for Handling Sport Issue. Journal of Sensors, (11), 1-12. DOI: 10.1155/2016/1814264.