# Double Authentication Model using Smartphones to Enhance Student on-Campus Network Access

Zakaria Saleh[1], Ahmed Mashhour[2]
Information Systems Department
University of Bahrain
Al-Sakhir, Bahrain

***Abstract*—Computers are widely used by all universities to provide network access to students. Therefore, the securities of these computers play a major role in protecting the network. In light of that, a strong access control is required to ensure that sensitive information will only be accessed through firm authentication mechanism. Smartphones are widely used by students, and can be employed to further enhance student authentication by storing partial access information on the Smartphone. And while students should not leave their computer systems unattended, some do. Therefore, daily network access requires that computer unit to be configured in a way that includes password authentication and an access code stored on a device (the smartphone) which needs to be presented by the user during the authentication process. It is a fact that software and hardware may fail to fully secure and protect systems, but user's negligence to safeguard their systems by logging out of the computer unit before moving away is far more serious security issue. The system being developed in this research will lock the computer unit once the student moves away from that computer unit and loosing communication with the smartphone.**

***Keywords—Bluetooth; double authentication; campus network; computer unit security; model design; smartphone; system design***

## I. Introduction

During the last few years, there has been a range of cyber security threats on university campuses worldwide such as phishing, ransomware, malware, and hacking. According to Urrico [1], Higher education institutions continued to see a high proportion of breaches and these threats are expected to rise significantly in the next decade. These threats are alarming for major information security risks in higher education according to Poremba [2], where many universities in the U.S reported data breaches that are caused by hackers infiltrating the college networks, and professors misplacing laptops that stored years of worth of student records. And according to the same report healthcare organizations, an industry that shares copious personal information, the breaches account for 42% of all industry incidents in the first 6 months of 2016, where breaches are caused by unintended disclosure.

In general, universities are being accessed on daily basis by thousands of students, how would brows the institutional data every single minute. All campus network systems, are vulnerable to different kind of security risks, and one of the major vulnerabilities comes directly or indirectly from the student. Implementing a robust access control is a great way to protect campus network and preserve the confidentiality of data it maintains. In this research we believe that the access control should be "something the user has" and capable of continuance interaction with computer unit being accessed, and continue to maintain control even after the network access is authorized. This means that when a student wants to leave the computer unit without logging off, even if he/she plans to comeback, a firm security system calls for ceasing access the computer unit during the student's absence. This paper will focus on student authentication and control to allow authorized students access to campus network and deny a walking-by student the opportunity of finding a logged on but unattained computer unit. Typically, logging on to campus networks require a student to provide an ID and password and then go through the identification and authentication process to confirm the identity of a student. This study presents an enhancement to that method through the use of double authentication model capable of reliably identifying students before and after accessing the campus network.

## II. Significance of the Study

Securing desktop computer units is a significant part of the network and information-security strategy in any organization including universities because of the sensitive nature of the information often stored in an organization or university databases. These databases are visible into the Internet and exposed to attacks because they are heavily accessed by staff and students, and as well as the temptations for an unhorsed student of the account to misuse a logged on but left unattended by the authorized student.

Different surveys on security breaches identified several challenges. The SANS Institute [3] conducted a computer security survey on universities and colleges (junior and community colleges), were data was collect from around 300 Information Technology professionals, where (87%) are placed at United States institutions , and 13% from other part of the world. The results show that about 70% of participant expressed worries about the university systems that stores data about students and financial records, and 64% of respondents were concerned about the networks computer units as well as laptops used to access the network [3]. Moreover, Brumfield [4] in Verizon Data Breach Investigations Report, which analyzed security breaches and reiterates the need of organizations for basic security checks in order to protect their data need to know what attack patterns are most common for their business, apply two-factor authentication for their systems and applications, review their logs to help identify malicious activity, encrypt their data and train their staff to developing security awareness within the organization. The report recorded more than 100,000 security incidents, indicating a 23% increase compared to security breaches in year 2015. Fig. 1 summarized the identified breaches and their relative incidents.

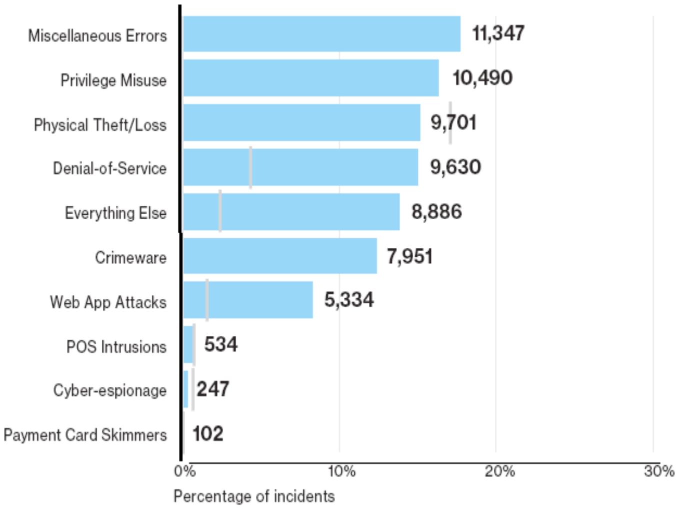


Fig. 1. Incidents and breach breakouts for 2015 (Source: Brumfield [4]).

A report by VMware [5] explored the extent of cyberattacks and the IT security standards used within UK higher education institutions. It also investigates the steps universities can take to protect their intellectual property against today's increasingly sophisticated threat landscape. The report concluded that attacks on student data are common. Over a third (36%) of UK universities are blighted by a successful cyberattack each hour. 43% have had student data attacked, including dissertation materials and exam results. 25% have experienced critical intellectual property theft. 28% have had grant holder research data attacked

Two-factor authentication delivers authentication through devices the users have and the information (such as Pin Code) they already known. Financial institution have applied double (i.e. two-factor) authentication successfully with credit cards and mitigate the rate of breaches of their customers' transactions. Credit card has helped the banking sector to offer security and privacy to their customers because it is reliable, available, and efficient [6].

Smartphones have become an integral part of everyday student's life [7]. In this research we propose using Smartphones and Bluetooth technologies as a second authentication device to minimize students and school records unauthorized access. In light of that, two-factor authentication (2FA) becomes a necessity in higher education transacting to protect against security breaches of higher education sensitive data such as student records, research records, intellectual property records, and so forth. Two factor authentications were recommended by Cristofaro [8] which aims to enhance resilience of password authentication factor. Their research identified popular 2-factor solutions including one time code generated by security token, and one time PINs received by email or SMS and dedicated to smartphone Apps. The two-factor technologies are perceived as applicable regardless of motivation and/or context of use and no gender differences in terms of adoption rate for token and email/SMS. Digital signatures are usually used by trusted authorities to make unique bindings between a subject and a digital object. Poettering and Stebila [9] proposed a type of signatures called double-authentication-preventing signatures, where a subject/message pair is signed. This is in order to provide self-enforcement for correct signer behavior and provide greater assurance to verifiers that signers behave honestly.

## III. Literature Review

According to Kecia [10], in Spring 2017 issue of Converge journal protecting student data are never-ending cybersecurity concerns. It should focus on highlight the role played by technology in modern education by examining networks cybersecurity and data privacy. The study explores two U. S. states where laws have been passed to protect student data including Colorado and Connecticut. It identifies the challenges and possibilities of ensuring student data are protected within the requirements of the law while at the same time enabling school officials to utilize student data for decision-making. In Colorado for example, one main problem to solve is how schools balance student privacy while encouraging teachers to find Apps and Web tools that support their classrooms. In Connecticut State, some of the measures used is Information Technology team provides iPads for students and controls which apps they can access. Principals and curriculum directors have protocols to follow to make sure that educators go through the Technology Department for approval Data and Privacy Council, which developed a student data privacy toolkit that helps them effectively implement the new data privacy legislation Indiana.

University provides students at campus access to two separate secure wireless networks one for academic work, and another for gaming and other extracurricular activities. A recent study by BitSight Technologies [11] report, malware infections increased by a high percent close to 48 percent on the U.S colleges' campuses last year and BitSight Technologies [11] report reveals that as a sector, top schools are at even greater risk for security breaches than retail stores and healthcare. Educause [12], in a nonprofit association whose mission is to advance higher education through the use of information technology, listed information security as the number one issue facing higher education in 2016 and 2017.

In today's schools environment, the need exists to ensure that only authorized individuals gain access to critical devices or services offered. Two-factor authentication (i.e. double authentication) solution equips students with a cost effective means of providing flexible and strong authentication to very large scale, diverse audiences both inside and outside school campus.

Examining networks cybersecurity and data privacy Rasmussen [13] believes that the majority of universities' records of research, financial administrative, and clinical are being access via the university's network. In addition, almost all records on student information, medical information, library use, research, as well as intellectual property-related information are being stored on university servers, which make the network vulnerable to security major breaches by unauthorized users that could gain access to sensitive and or confidential information and expose the university to financial and reputation losses and other risks posing a threat to future admission, and financial strength. Although universities have lower financial loss rates than the industrial sector their risk managers face the intimidating challenge of identifying and managing the complex and growing risks across their campuses [14]. In the United States alone, security risks have effected more than 200 colleges and universities according to Rasmussen [13], indicating that educational institutes lost control of files in the amount 22 million, which contained detailed information about important research projects, as well as students' personal information such as social security numbers and financial information.

## IV. Bluetooth Overview

Bluetooth is a wireless communication technology that was designed and implemented at Ericsson (in Sweden) during 1994. The technology was originally introduced as a method to connect devices to computers and laptops without the need for overcrossing cables. Because of the unlimited potential of Bluetooth wireless communication, Ericsson and other companies (IBM, Intel, Nokia, and Toshiba), established the Bluetooth Special Interest Group (SIG) in February 1998. SIG objectives were to develop an open specification for short-range wireless signals that can be used for connectivity [15]. Bluetooth Specification IEEE 802.15 was then developed so that so that BWT-enabled devices from different manufacturers can work together.

Bluetooth is a packet-based protocol, based on the master-slave structure, and operates within the Industrial, Scientific and Medical (ISM) communication band of 2400 to 2483.5 MHz. A Bluetooth Adapter is capable of performing several tasks. The Adapter can initiate device discovery, it can query a list of paired devices, and create an instance of Bluetooth communication with devices using a known MAC address, and create a listening BluetoothServerSocket that's ready for incoming connections requests from other devices. In addition, the Bluetooth Adapter is also capable of scanning for Bluetooth devices. The master-slave concept within the Bluetooth technology makes the unit that starts a communication link as master and the units that respond to the request as slaves [16]. Such functionalities can be a perfect feature for the proposed Smartphone authentication Logon system.

## V. An Overview of Computer Unit Security

The main objective of network security is to deny unauthorized users to access the network or a network computer unit. Colleges and universities are safeguarding their networks to ensure that students access only the information and network resource they are approved to access. Furthermore, access control methods are utilized to ensure that authorized students are not denied access to resources that they are permitted to access. Procedure for securing unattended computer requires students to turn off computers or logout at the end of the session or set to hibernate when a student will walk away for an extended amount of time with the intention to come back to the same computer. While Computer units are safeguarded from unauthorized access, and shall never be left unattended. However, it has been noticed that many unattended computer are accessible after the end of session, because none of the security measures were taken by the students to either logout or hibernate the computer. Security was primarily achieved by controlling physical access to system components which were unique and used proprietary communication protocols [17].

Modern methodologies and approaches in the formal education sector used to improve students learning experience are all based on the use of information technology, therefore, institutions in higher education are paying more attention to information technology to deliver and enhance students' knowledge and skills. However, producing and maintaining a convenient and secure campus network system is a challenging task. Universities tend to have a weak centralize policies, which means that they have the tendency toward decentralization where in some universities different departments have their own network equipment, staff and budget [18].

Universities and colleges are being views as good potential targets by data hackers, resulting on and increased security attacks on these institutions [3]. There are three main security issues related to securing a computer unit: Confidentiality, Integrity, and Availability. Information stored on the university servers may be disclosed inappropriately. This can happen for example, when unauthorized students gain access to the unattended computer, and therefore, authorized students gain access to information that they are not supposed to see, or authorized students inappropriately transmit information via the network. The integrity of personal information stored on the server may be changed maliciously (e.g. withdraw from a class). Authorized students may be unable to use the network when the information has been damaged, deleted, or otherwise rendered inaccessible (e.g. having its access privileges changed).

According to Al Maskari [18] identified several vulnerabilities of the unauthorized access to, which includes:

- Ability to executable commands without prior authentication.
- Unauthorized access to data by authorized users.
- Impersonating another use or service within a system.
- Accidently or intentionally causing a denial of service attack.
- Modifying or removing contents without permission.
- The effort to exploit encrypted data and information.

## VI. Proposed System Design

The present education system, with the advancement of information technology, the objective is to provide students the abilities to access information. As it is evident, the Internet can offer students the gateway to access information and educational materials in different formats, ranging from electronic textbooks, to other interactive models of learning environments. Colleges and universities are increasingly providing students access to information sources through their campus networks. The campus network is typically recognized as that part of the computing structure that supports access communication services to resources for users including students. In many cases the network covers a group of buildings located throughout the campus geographic area. In some cases, the network could include a distinct campus that would act as the central/backbone of the network that is designated to support interconnectivity between the different segments of the entire network. To access the campus network, the current methods are based on identity registration along with a passcode recognition, where the system assume that the users' identity is a subject to ethical actions. However, statistics accumulated for many years indicate that the major security breaches are caused by trusted, identified, and legitimate users [19]. An access control mechanism imposes selective restriction of access for the users or any process being executed for the users, consuming, entering, or using network resources, like application programs, files, and databases.

The proposed access control system, is intended for controlling access during an access session by a user, and mediates between the students and the network components and services that students are permitted to access, as specified in the standard access control policy and the availability (i.e. presences) of a smartphone running access approval application. Campus Access Control systems (see Fig. 2) will provide the necessary steps needed for identification, authentication, and authorization (access approval), as well as students' accountability by specifying what a student can do. Moreover, while identification and authentication are the standard means to ensure that only legitimate students will be able log on to the network, the proposed system besides the network access control (NAC) system can be a useful technology in providing an enhanced access control. When used together, a combination of NAC and proposed system will provide stronger security and operational safeguard.

For testing the proposed system, we have developed a code to implement the smartphone authentication Logon plug-in to be used on the server to configuring the server and enable it to use the smartphone authentication Logon concept. As for the computer units, for using the extended Smartphone authentication method, there is a need to install the extended application. Conveniently, interacting with Bluetooth communicators available on smartphones is not complicated, and Windows operating systems come with tools for Bluetooth Technology support.

Fig. 3 illustrates the general process of the suggested authentication system. A Bluetooth Adapters is needed for the computer unit to enable students to logon, providing that the smartphone (own by a student) is within the transmission distance of the Bluetooth. Once the student enters the ID and password, and a match is found in the database, the system will attempt to associate the user with a pre-registered smartphone by sending request for the smartphone's MAC address so that the returned value can be compared with the data stored in the database. The logon is based on Single Sign On (SSO), and the student is only asked once to enter the ID and password, a periodic request is set for smartphone's MAC address. The student will be logged off if the smartphone fails to reply, assuming that the student has left the computer unit without logging off (the detailed process is explained in Section VII, Proposed System Design.

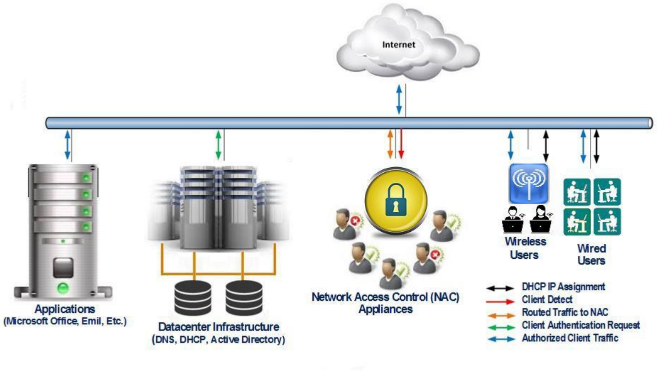

Internet
Applications
(Microsoft Office, Emil, Etc.)
Datacenter Infrastructure
(DNS, DHCP, Active Directory)
Network Access Control (NAC)
Appliances
Wireless
Users
Wired
Users
DHCP IP Assignment
Client Detect
Routed Traffic to NAC
Client Authentication Request
Authorized Client Traffic

Fig. 2. Campus access control systems.

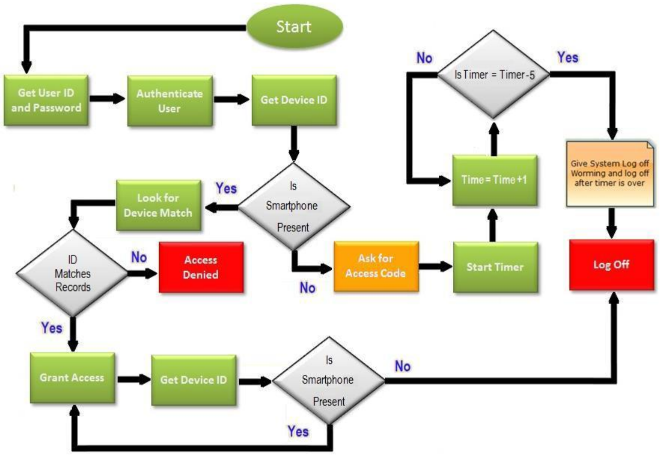


Fig. 3. A simplified process for the proposed authentication Logon.

Sometimes users in general, and students included, avoid locking commuters when walking away from the computer unit, because it is more convenient for them than having to type passwords again and again. In light of that, the solution is to have an interactive program running in the background that automatically detects the presence of the user's smartphone. The communication between the smartphone and the computer unit is recommended to be encrypted to ensure that the communication signals are not going to be read if intercepted by someone who maybe intentionally listing for such communications that carries critical piece of sensitive data. However, during our testing of the system, we did not apply any encryption because we were testing in a lab setting, were such information is out of reach for anyone outside the testing environment.

## VII. Proposed System Design

### A. *Configuring the Server*

In order to enable the use of the extended Smartphone authentication method, we have developed an extended Smartphone authentication Logon plug-in. The plug-in will provide three main functions: 1) Bluetooth device name and user ID matching; 2) Smartphone removal responses; 3) update the windows Logon to include a smartphone based Logon. Therefore, there is a need to install the extended Smartphone authentication Logon plug-in. When installed, the System Administrators use this plug-in to configure settings for global (general), or individual users. The global settings can be used to specify access policies for the entire network. One the installation is completed and the system is up and running, the sever can be configured to apply the Double Authentication, by registering one smartphone for each student. When a smartphone is registered, each smartphone will be assigned a Bluetooth device name, and the name will be bonded with the student ID (of the smartphone owner). Precaution are being made in the extended Smartphone authentication Logon plug-in, to allow for a temporary none existence of smartphone-student ID bonding (the period is flexible for ease of use of the system).

### *B. Bluetooth Device Name and user ID Matching*

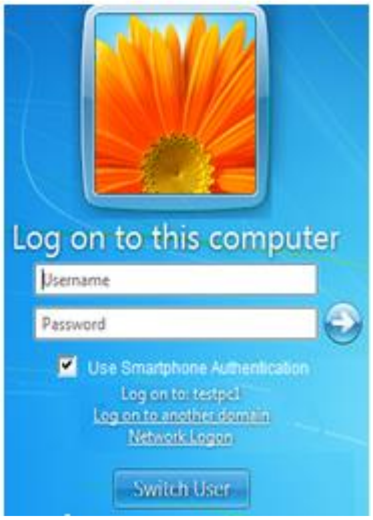
When a student attempt to logon, the smartphone needs to be present, and during the Logon, there will be Bluetooth device name matching process to verify if the Bluetooth enabled smartphone presented during Logon is matched to the targeted student account. There are three options: Student Name matching, which will check the device name presented during the Logon against the device name stored for the student smartphone. Matching device name is required to approve access. No Matching means no device name during the Logon process is needed on the target student account. Typically, this option should not be used as the default student accounts. However, when required, access will be allowed for a specific period of time. This will be explained in more details under “Setting up Smartphone Based Windows Logon”.

### *C. Smartphone Removal Responses*

Smartphone removal response defines the action taken when a student removes the smartphone away from the Bluetooth reader (Smartphone removal assumes that the student is walking away from the computer unit). In this case, extended Smartphone authentication Logon plug-in application locks the computer unit. If the student smartphone does not become available after a period of time, a “Forced Log Off” will be administrated by the Logon plug-in application. This setting should be used with caution because it can result in the student losing work when the forced logout occurs, so the time for “lock the computer”, should not be very short, since no one else can access the account during that period.

### *D. Setting up Smartphone based Windows Logon*

The Smartphone Authentication for Windows Logon support will allow the smartphone to be used for a computer unit login. To enable the Smartphone authentication for Windows Logon feature, the student user will need to check the box that indicates the Use Smartphone for Computer unit Login. This requires the presence of the students’ preregistered Computer unit Login Smartphone as per the security requirement of Windows Logon (see Fig. 4). If the student does not have the preregistered Computer unit Login Smartphone, or the phone is not functional (for any reason), then the student does not need to check “use Smartphone for Computer unit Login” box. In that case, per administrator’s imposed access control policy, may grant a temporary access, and before the time is up, a warning message may be displayed asking student to save all data, due to a system administrated log off.



☑ Use Smartphone Authentication

Fig. 4. Windows logon with smartphone authentication support.

## VIII. Experimentation and System Assessment

A prototype was developed to determine the systems usability; we implemented the system and developed simple experimental software for the smartphone authentication using a Bluetooth adapter and an Android smartphone. The prototype implementation exhibited the major functional capabilities including 1) establishing communication; 2) requesting smartphone MAC address; 3) continually pinging the smartphone to determine its existence; 4) a function to automatically lock and turn off the screen of the computer unit, and then start the timer; 5) a function for automatic log off when the timer is over.

In the prototype software runs at windows startup as a service that is continuously in a listening status. As soon as users checks the box that indicates the Use of smartphone for Computer unit Logon, the smartphone information are retrieved from the phone and sent to the Access Control in Database Management Systems, which provides access rights to the network. Once the students’ identity is verified, the students’ relevant access authorization is granted to the student.

## IX. University Campus Lab Simulation

A small network (which contained seven nodes), was implemented so that the suggested design of the smartphone authentication system can be tested. On system was assigned the server role, and the database contained 10 user accounts, where only six accounts were bonded with smartphone manually in the database. All test computers were seated in one room of an area of 6 by 8 meter. The computers were about two meters apart. Number of users assumed of no consequence of the tests finding. Besides the number of test computer elements, speed of transmission, the distance of device connectivity, and data quantity were the main qualities selected in the simulation. Those three elements were being adjusted during the system simulation test, because they have a direct effect on each other and the overall findings of the tests. Communication distance for the USB Bluetooth devices was assumed to be with 7-8 meters due to assumed added interference and obstructions, but during the test experiment going as far away from the device as possible, we found that none of the systems stayed logged on after about 10 meter range. For the testing simplicity and due to the fact that data quantity is not a major issue in the access confirmation scenario (i.e. one user account was tested at a time), however is different from real life implementations such as several lab rooms where larger volume of data would be transmitted during the authentication of multiple students. In the other hand, speed is significant, so the response time during the test simulation was set in seconds to ensure speedy logging on, due to the fact that the real system would be receiving a much more logon request, and a slow response could affect the overall network access. Three different types of test were conducted: the first one was to test the functionality of the extended Smartphone authentication Logon system by trying to logon during the presence of the smartphone, and then moving the smartphone away from the computer; the second testing was by logging on using the accounts that were not bonded with smartphone to insure that this function works as intended, and the third test was conducted using the accounts that were bonded with smartphone, but the smartphone was not present during the logon. Some modification was made to extended Smartphone authentication Logon plug-in, to resolve some minor issues that were experienced during the system testing. At the final stages of the testing, all tests conducted on the system were fully successful and the functional.

## X. Conclusion and Future Work

College campus is a heaven to thousands of smartphones and computing devices with open, easily hackable Wi-Fi coupled with Students careless or unawareness of digital privacy and security. Using two-factor authentication scheme probably is a partial solution to intractable security problem in a college campus. In this paper, we proposed a second layer authentication system using smartphone to enhance campus network access, which in turn will add a second security layer which combines logical software security (something the user knows) with a smartphone Bluetooth identification (something the user has). Combining what the user knows with what the user has, while the objective of this research is to ensure a log off when a student walks away from the computer unit, the indirect benefit would be an improved security structure of the campus network access systems while at the same time, there were no indications that it would impact the system performance in a negative way.

Smartphone Authentication Logon access control system, as it has been illustrated during our implementations and testing, can be easily installed in the current system with no need for considerable added components in terms of hardware or software. A simple prototype and simulation were developed to establish the feasibility and usability of the proposed system, by evaluating the major functionalities as well as the characteristics that determine selecting the Bluetooth reader in terms of response and communication distance, and all tests conducted on the system were fully successful and the functional.

## References

[1] R. Urrico, (2016). Malware Attacks Targeting Smaller Financial Institutions, Credit Union Times, july 20, Retrieved from http://www.cutimes.com, (in June 30, 2017)

[2] S. Poremba, (2014). 5 Higher Education Information Security Threats You Should Know Before Your Child Leaves for College. Retrieved from, https://www.forbes.com/sites/sungardas/2014/11/05/5-higher-education-information- security-threats-you-should-know-before-your-child-leaves-for-college/#7c7788dd1239, (in April 15, 2017).

[3] R. Marchany, (2014). Higher Education: Open and Secure?, SANS Institute, A SANS Analyst Survey. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/higher-education-open-secure-35240. (in May 10, 2017).

[4] J. Brumfield, (2016). Data Breach Investigations Report finds cybercriminals are exploiting human nature. Retrieved from http://www.verizon.com/about/news/cyberespionage-and-ransomware-attacks-are-increase-warns-verizon-2017-data-breach ( in June 30, 2017).

[5] VMware (2016). University Challenge: Cyber Attacks in Higher Education. Retrieved from https://1f289b3qza8o3dim3uta9yl5-wpengine.netdna-ssl.com/wp-content/uploads/2016/06/36300-VMware-Cyber-Security-Report.pdf (in June 15, 2017), pp 1-12.

[6] O.S. Adeoye, (2012). Evaluating the performance of two-factor authentication solution in the banking sector, IJCSI International Journal of Computer Science Issues, July, Vol. 9, No. 4, pp.457–462.

[7] J.n. Alson, and L.V. Misagal, (2016) Smart Phones Usage Among College Students, International Journal of Research in Engineering & Technology, Vol. 4, Issue 3, pp 63-70.

[8] E. Cristofaro, P.J.F. Parc,h., and G. Norcie (2014). A comparative Usability Study of Two-Factor Authentication, The 18th Network and Distributed System Security Symposium (NDSS), Feb. 23-26, 2014.

[9] B. Poettering, and D. Stebila (2017). Double-authentication-preventing signatures, International Journal of Information Security, Volume 16, Issue 1, pp. 1-22, doi:10.1007/s10207-015- 0307-8.

[10] R. Kecia (2017). Are students data laws a blessing or burden? ,Executive Director, Center for Digital Education The Center for Digital Education, Convergence 2017.

[11] BitSight Technologies (2014). Powerhouses and Benchwarmers: Assessing Cyber Security Performance of Collegiate Athletic Conferences, BitSight Insights Report . Retrieved from http://bitsig.ht/1oX0Lm8 ( in May 20, 2017).

[12] Educase (2017), Educause leadership strategies computers and network security in higher education. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/higher-education-open-secure-3524, ( in August 3, 2017).

[13] R. Rasmussen, (2011). The College Cyber Security Tightrope: Higher Education Institutions Face Greater Risks. Security Week, April, 28, 2011.

[14] M.A. Bubka, (2010). Best Practices in Risk Management for Higher Education. Retrieved from https://www.pmacompanies.com/pdf/MarketingMaterial/PMA_Education_BestPractices_WhitePaper.pdf ( in July 22, 2017).

[15] K. Sairam, N. Gunasekaran, R. Redd (2002). Bluetooth in Wireless Communication, IEEE Communications Magazine, Volume 40 Issue 6, pp. 90-96.

[16] S. S. Chadha, M. Singh, and S. K. Pardeshi (2013) Bluetooth Technology: Principle, Applications and Current Status, International Journal of Computer Science & Communication, Volume 4, No. 2 September, pp.16-30 ISSN-0973-7391

[17] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart (2016) A review of cyber security risk assessment methods for SCADA systems, Computers and Security 56, pp. 1-27.

[18] S. Al Maskari, D. Saini, S. Raut, and L. Hadimani (2011). Security and vulnerability issues in university networks, Proceedings of the World Congress on Engineering (WCE), Vol 1, July 6-8, 2011, London, U.K.

[19] Almehmadi, and K. El-Khatib (2015). On the Possibility of Insider Threat Prevention Using Intent-Based Access Control (IBAC), Systems Journal, IEEE , vol. PP, no. 99, pp. 1-12.