

Security Measures Implementation on the Web Access: University's Turnstile Interfacing

Donneger P. Grancho¹, Florence Jean B. Talirongan² & Hidear Talirongan³

^{1,2}Misamis University, Ozamiz City, Philippines.

DOI: <http://doi.org/10.46382/MJBAS.2021.5103>

Copyright: ©2021 Donneger P. Grancho et al. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Article Received: 19 October 2020

Article Accepted: 03 February 2021

Article Published: 12 February 2021

ABSTRACT

As technology keeps on upgrading, organizations were also challenged to adopt new trends. Higher education institutions (HEIs) were looking into the security measures of the technologies used in the university or colleges to secure important data as an important asset in the organization. The study addressed the security issues in terms of internet access through interfacing turnstile and web captive portal of the university. Only those currently enrolled students who pass the turnstile and who has an account in mymu server can successfully access the internet since the student will just be using one account for the mymu account and captive portal.

Keywords: Access control, Internet security, Turnstile, Captive portal, Web access.

I. Introduction

Technology plays a vital role in the advancement of higher education institution and will continue to have a significant impact on higher education. Significantly, students become more engaged in constructing knowledge in technological innovation that will come to class armed with smart phones, laptops and iPods [1]. Connection to school's wireless network is available throughout the campus where the student can use their wifi-enabled devices to connect to the internet. To access the network, a captive portal is shown wherein it is a web page that the user of a public Wi-Fi network view and interacts with the portal before they are allowed to connect and it can be designed in many different ways. It can be in a form of a log-in system with a pre-designed user ID and password for a fixed amount of time to access the network. The need of protecting and securing user information authentication is increasing [2, 26]. Many institutions of higher education are accelerating efforts to implement technology in support of the learning process [3]. As institutions of higher education continue to roll out online courses and programs, issues of undergraduate student readiness on the one hand, and the challenges surrounding the design and development of pedagogically-sound online experiences that are also accessible to students remain of concern [4]. The internet, as a context of social change and identity information, can create cyberspaces for governments in exile, such as in Tibet [5]. Internet use among students in tertiary institutions in the Sunyani Municipality, Ghana is more focused on using the Internet technology to look for information for assignments [6]. Same study in University of the Punjab, Lahore shows that most of the students use this technology for course related reading and research needs. They use it at the University Library's Digital Lab Unit as well as their departments and homes [7]. Awareness and usage of computer and internet among medical faculties' students at the University of Jordan resulted that most medical students have average 5 or advance knowledge on the basic use of computer and internet. Google was found to be the most commonly used search engines. Also the study found that ICT (Information and Communication Technology) can be a useful tool in medical education but the lack of time,

internet connectivity and resources is still a serious constraint [8]. A study on the development of a framework for the use of e-learning in teaching industrial, technical education in Nigerian Universities resulted that infrastructure is required for e-Learning as well as its access and use [9]. United States institutions implement Massive Open Online Courses (MOOC) which provides an opportunity to expand access to postsecondary and adult education to expand their course offerings via online programs [10]. The university uses a captive portal intended to provide services to students and employees to access the Internet within the campus. The Misamis University's Portal requires them to fill in the id number and password in order to access the internet connection. However, even if the students will not enter the campus as long as they are in a nearby area of the WiFi hotspot, they can still access the internet connection. Another concern is the existence of intruders that allow other student to access another account. With that, this research will help in the implementation of security measures in the control of web access by connecting the turnstile data to the captive portal.

To access the network, students must authenticate using the captive portal feature. The authentication process happens when the student logs in the username and password. It is still considered as a weak security measure since intruders can access others' account. Thus, the study interfaces the ease of access of the students to Misamis University's portal with the university's turnstile at the entrance gate.

With the existing turnstile system, only the enrolled students can enter the campus provided that the identification card is validated for a given semester. Once the student is inside the campus, he or she can access the internet provided that he or she is successfully registered with the captive portal. However, even if the students will not enter the campus and who are living near the school where there is an internet connection, he or she can still access the internet.

Given the above situation, the researcher would like to address the following problems:

- security of the internet connectivity usage exclusive only to those students who are currently enrolled in a given semester who are currently inside the campus and passes by the turnstile system of the University by designing the interface that connects the turnstile technology to the university's portal; and
- security on the account of student's username and password might be used by intruders in order to access the Internet.

The main objective of the research is to interface turnstile and the captive portal of the University in order to address the security issues in terms of Internet access of the University.

Specifically, it is also designed:

- to retrieve students' data who pass from the turnstile;
- to configure a captive portal server that will link the students' profile data from the my.mu.edu.ph server (mymu account) and turnstile database;
- to allow Internet access using authentication of the student who pass through the turnstile.

II. Related Literature

Security is one of the major issues which played an important role in the use of the web portal. Access control is the process of mediating every request to data and services maintained by a system and determining whether the request should be granted or denied [11]. It has been in use for years, which is used to restrict the access of unauthorized devices [12] so that only the registered devices can use the given internet. In the present situation of the university, there is an existing turnstile system that restricts the passage only to students who are currently enrolled in a given semester and whose identification cards are validated. A study was conducted by Brooks [13] in Central Michigan University and Chen [15] on the use of web portal for its students, staff and faculty accomplish important tasks. It was found out that the first time users were more likely to have issues with navigating the portal than the users who have used it before the study. Smith [14] and Liao et al. [25] used the technology acceptance and information systems success models for the use of the university library Web portal. The result indicated the positive effect of user satisfaction on use increased and impact on the intended use of web portals. Nambiar et.al [24] discloses a method and network device for maintaining captive portal user authentication that allows client devices to access a network that requires completion of a portal web page [16] and even redirecting the users to given URL (Uniform Resource Locator) [17]. A method, apparatus, and system in which a module may have both an Embeddable portion and a cooperating downloadable portion scripted to plug in and be integrated into an existing Terms and Conditions page of a public Wi-Fi and/or wired network. The module is scripted to direct the web browser [27] back to the Terms and Conditions page once the web browser on the client device has been through the third-party captive portal and authentication flow and its associated one or more web pages that are parsed and rendered by web browser [18].

The study of Bar [19] presented a system that includes a mobile device, a handover device, a network, a captive portal server, and an application server that may interact with a handover device to automatically connect to the network. Once connected to the network, the captive portal server may connect the mobile device to a captive portal. Leaving the restricted area allows disconnection of the user from the Internet. A device may be off-line at various instances. For example, in a “captive portal,” a mobile device may be connected to a WiFi signal but the mobile device is not authenticated. As a result, the mobile device acts as if it were off-line in some scenarios [20].

A study of Captive portal by Venkiteswaran and Calamari [21] directs a guest user on a network to a special browser web page that is typically used for authentication or payment purposes before allowing the guest user to use the Internet [28]. However, devices like Chromecast™ and Apple TV™ do not have any browser functionality to allow them to connect or authenticate to the special browser web page presented by the wireless network.

Canning [22] studied educational environment in which an outbound proxy is used to allow teachers to access a web site (e.g., YouTube or Facebook. However, users can access the wireless network but are required to authenticate to access the Internet (via a captive portal). In the study of Scherzer [23], the availability of an alternative wireless network can be determined, in many instances, access to the wireless network is controlled through the use of encryption, access password and captive portals. This means that users must ask for permission to access and use the network.

III. Research Framework

The researcher utilized the developmental research method in which the design-development process is accomplished using Systems Development Life Cycle (SDLC) Methodology used by Chakraborty et al. [29] with modification. Generally, an SDLC Methodology follows these steps which will address the problem stated in this study: (1.) If there is an existing system, its deficiencies are identified. Recently, Misamis University has its turnstile system where the students will pass by before coming inside the campus and captive portal system that allow the users to access the Internet. Presently, students who have wifi enabled devices can access the Internet by filling in the username and password found in the captive portal. However, those students who are living near the campus can still access the Internet even if they are not inside the school premise. In addition, the students can also access other students account as long as they know their username and password. (2.) The new system requirements are defined. To fully implement the security of the Internet access exclusive to students of Misamis University, the researcher will utilize the two existing systems by creating a program that will link the profile data of the students who pass through the turnstile to the captive portal so that only those who pass the turnstile can truly access the captive portal. (3.) The proposed system is designed. Plans are created, including programming and security issues. (4.) The new system is developed. The new components and programs must be obtained and installed. (5.) The system is put into use.

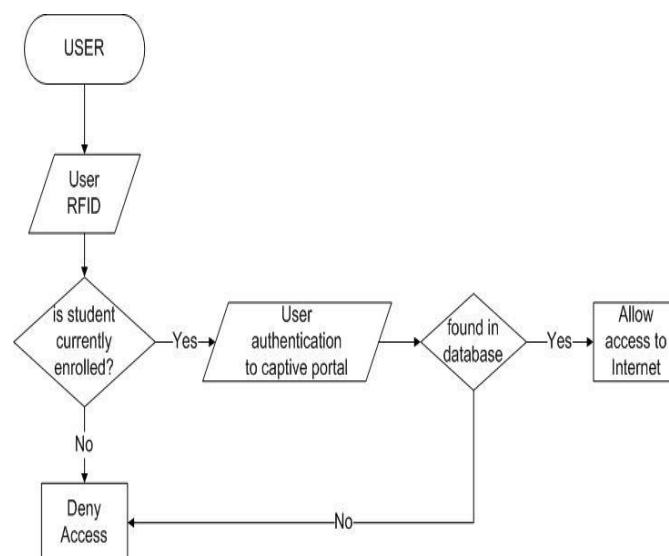


Fig.1. The flowchart of allowing Internet access

The flow of the proposed system is presented in Figure 1. It illustrates the process where the user referring to the students will use their radio-frequency identification (RFID) card to check whether the student is currently enrolled or not. If currently enrolled, the student will authenticate his or her account in the captive portal. If the student's profile data coming from the turnstile is found in the database, the student can then access the Internet; otherwise, Internet access is denied. The design processes included the architectural design and the detailed design of the developed system on interfacing turnstile and the portal with security measures implemented. The architectural design is reflected in Figure 2. The flow starts from left to right picture wherein it presents the

students' data who will pass first in the turnstile. The turnstile system can only recognize currently enrolled students of the University which is imported from the mySQL database coming from the Registrar's Office. The data in the turnstile was extracted using a ZK Software Development Kit (SDK).

With the implementation of the system, the researcher use VB.net in order to send message to the my.mu.edu.ph server those who successfully pass the turnstile. Using the radius database, it will store the students' data who successfully registered the mymu account and passed the turnstile. From my.mu.edu.ph server, it will then send message to the captive portal server to allow student to login the captive portal and access the internet. The server task program is capable of authenticating the students' profile data coming from the turnstile system. Additionally, it is also the task of the server to inform the students, especially if his or her Internet access is denied. For the internet use, the wifi enabled devices are used by the students to access the Internet. If the students profile data is found in the turnstile system, students can successfully access the Internet. Implementing security measures on the Internet access is very important in order to avoid intruders who will be using other students account and to make the Internet access of the University exclusive to use inside the campus.

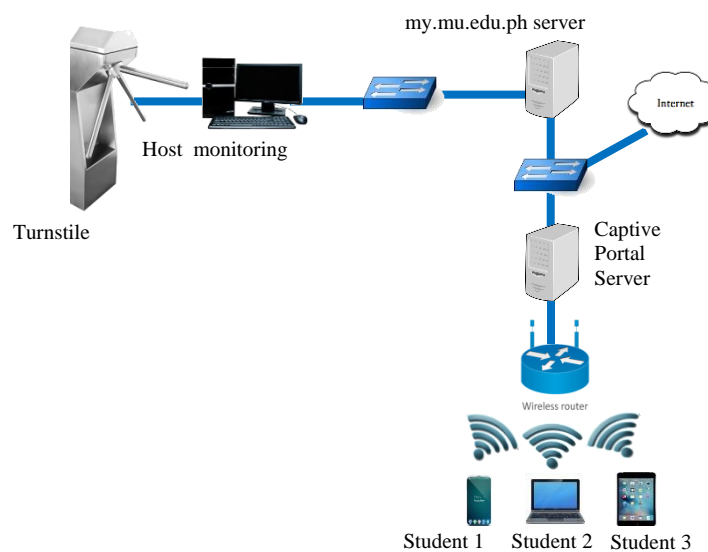


Fig.2. Architectural Design of the Proposed System

IV. Results and Discussions

Internet security is an important area of concern in every organization. In Misamis University, there is an existing turnstile technology that allows the students to pass during school days and there is also a captive portal that allows the students to access the internet. However, in order to fully implement the security issues in terms of the exclusive use of the internet in the university and to avoid the intruders of using the internet, the study will interface the turnstile technology and the captive portal system. The system started the process when the students pass the turnstile. Only those who are currently enrolled students can pass the turnstile. Turnstile has RFID that can detect student's ID which also contains RF number. Students RF number is unique which was validated by the Registrar's Office during enrolment process. Figure 3 presented the graphical user interface of the student who successfully passes the turnstile.

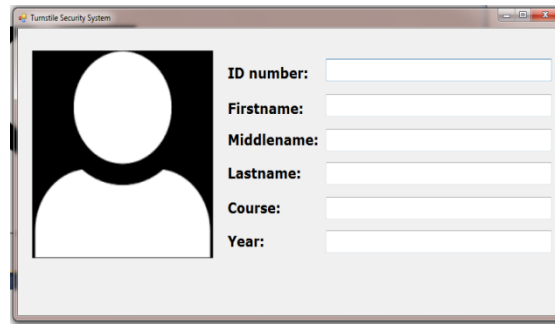


Fig.3. Graphical User Interface of Student

Figure 4 presented the visual basic code that will manipulate PHP codes found in my.mu.edu.ph server. The purpose of having this code is to invoke the PHP codes that manipulate the captive portal users. The subroutine add_user with idno as an argument id number of the user and sends the data to my.mu.edu.ph server to be added as radius user for the captive portal. The subroutine del_users sends message to my.mu.edu.ph server to delete all the radius users of the captive portal.

```

Private Sub add_user(ByVal idno As String)
    Dim reqparm As New Specialized.NameValueCollection
    reqparm.Add("acct", "admin")
    reqparm.Add("idno", idno)
    Dim client As WebClient = New WebClient()
    Dim responsebytes = client.UploadValues("http://my.mu.edu.ph/add_user.php", "POST", reqparm)
    Dim responsebody = (New System.Text.UTF8Encoding).GetString(responsebytes)
    If Not responsebody = "ok" Then
        MsgBox("Cannot connect to server", MsgBoxStyle.Information, Me.Text)
    End If
End Sub

Private Sub del_users()
    Dim reqparm As New Specialized.NameValueCollection
    reqparm.Add("acct", "admin")
    Dim client As WebClient = New WebClient()
    Dim responsebytes = client.UploadValues("http://my.mu.edu.ph/del_users.php", "POST", reqparm)
    Dim responsebody = (New System.Text.UTF8Encoding).GetString(responsebytes)
    If Not responsebody = "ok" Then
        MsgBox("Cannot connect to server", MsgBoxStyle.Information, Me.Text)
    End If
End Sub

```

Fig.4. VB code that will manipulate PHP codes found in my.mu.edu.ph server

```

<?php
$acct = $_POST["acct"];
if ($acct == "admin") {
    $id = $_POST["idno"];
    $conn1 = mysqli_connect("localhost", "root", "12345678", "pro");
    if (!$conn1) {
        die("Could not connect: " . mysqli_error($conn1));
    }
    $sql1 = "SELECT * FROM student_account WHERE uname = '$id'";
    $result = mysqli_query($conn1, $sql1);
    if ($row = mysqli_fetch_array($result)) {
        $uname = $row["uname"];
        $pwd = $row["pwd"];
        $conn2 = mysqli_connect("localhost", "root", "12345678", "radius");
        if (!$conn2) {
            die("Could not connect: " . mysqli_error($conn2));
        }
        $sql2 = "INSERT INTO radcheck (username, attribute, op, value) VALUES ('$uname', 'password', '=', '$pwd')";
        if (mysqli_query($conn2, $sql2)) {
            die("Error: " . mysqli_error($conn2));
        }
    }
    mysqli_close($conn1);
    echo "ok";
}

```

Fig.5. Code in adding user to the captive portal

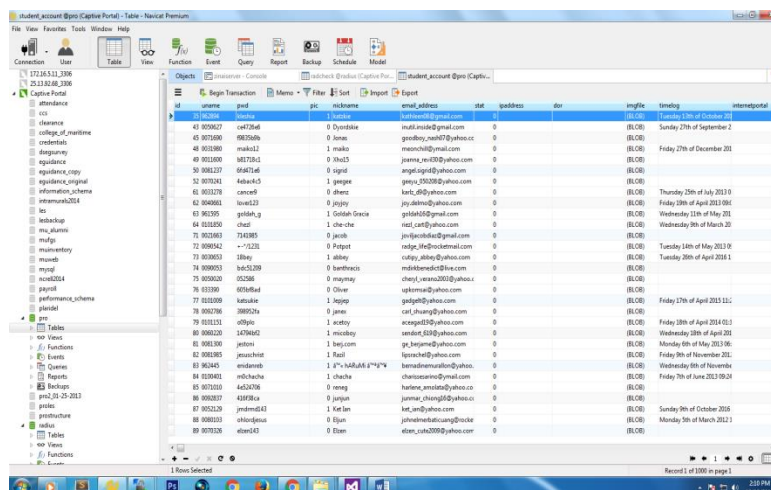
Figure 5 presented the PHP codes that will get first the username and password of the student from mymu account and insert to the radius database to allow access to the captive portal. Radius database was the storage of students who had an account in mymu and those students who passed the turnstile on a given day. Figure 6 presented the PHP codes that will delete all the users found in the radius database that was used by the captive portal. Every 5:00 in the morning, all users found in the radius database will be deleted so that new users will be inserted but only those who passed the turnstile.

```

<?php
$acct = $_POST["acct"];
if($acct == "admin"){
$con = mysqli_connect('localhost', 'root', '12345678', 'radius');
if (!$con){
    die('Could not connect: ' . mysqli_error($con));
}
$sql="DELETE FROM radcheck";
if (!mysqli_query($con, $sql)) {
    die('Error: ' . mysqli_error($con));
}
mysqli_close($con);
echo "ok";
}
}
    
```

Fig.6. Code in deleting all users from the captive portal

Figure 7 presented the sample database of mymu account that is used to send data to the captive portal so that student will only use one account in using the captive portal that is using their mymu account. This database presented the id number of the students as well as their password that is used in accessing the captive portal.



username	passwd	gtc	radname	email_address	stat	password	bar	login	timing	internetportal
43 905627	cat75a8	0	Dyostate	natul.muside@gmail.com	0	(BLOR)				Tuesday 23rd of October 2011
43 905580	9825266	0	Janece	gregory_west07@yahoo.co	0	(BLOR)				Sunday 27th of September 2011
48 905389	msk31	1	makab	monopol@gmail.com	0	(BLOR)				Friday 27th of December 2011
49 905200	MS17841	0	Xhu23	juanna_re03@yahoo.com	0	(BLOR)				
50 904227	9941145	0	sayid	angie.sigit@yahoo.com	0	(BLOR)				
52 905241	4sk4k5	1	angger	genya_0202@yahoo.com	0	(BLOR)				
61 903178	caac09	0	dherc	keri_b@yahoo.com	0	(BLOR)				Thursday 25th of July 2011 9
62 904961	kw4227	0	jayjay	joy.dhimo@yahoo.com	0	(BLOR)				Friday 29th of April 2011 9:01
63 902375	gsk4k_3	1	Golden Greca	patrick6@gmail.com	0	(BLOR)				Wednesday 12th of May 2011
64 931820	che21	1	che-che	risti_cari@yahoo.com	0	(BLOR)				Wednesday 9th of March 2011
71 902363	734395	0	javob	jin@rednet@gmail.com	0	(BLOR)				
72 909542	-*0223	0	Rastart	edgar_h@yahoo.com	0	(BLOR)				Tuesday 16th of May 2011 9
73 909063	18bay	1	abbey	ruby_abbey@yahoo.com	0	(BLOR)				Tuesday 20th of April 2011 1
74 909053	ba5229	0	banhravis	mdk@westcofire.com	0	(BLOR)				
75 909020	02286	0	angney	cheng_leeen02@yahoo.co	0	(BLOR)				
76 903390	60384af	0	Oliver	upkermal@yahoo.com	0	(BLOR)				
77 932289	katukate	1	keppp	gagp@yahoo.com	0	(BLOR)				Friday 17th of April 2011 11:1
78 902786	288202a	0	janee	cat_huang@yahoo.com	0	(BLOR)				
79 932151	o09pc	1	astory	acepaul03@yahoo.com	0	(BLOR)				Friday 18th of April 2011 0:01
80 904020	1479462	1	micokey	amont_82@yahoo.com	0	(BLOR)				Wednesday 28th of April 2011
81 902190	patem	1	baycom	pk_baycom@yahoo.com	0	(BLOR)				Monday 6th of May 2011 9:01
82 902385	jeusuhat	1	Raul	leptu4@yahoo.com	0	(BLOR)				Friday 9th of November 2011
83 962445	emidamb	1	*-k4L4N1 4742V	baradmenuraf@yahoo.co	0	(BLOR)				Wednesday 6th of November
84 923842	mlh3h3a	1	shacha	chenxuaner@gmail.com	0	(BLOR)				Friday 7th of June 2012 19:24
85 9071010	4453706	0	weng	harlene_arnita@yahoo.co	0	(BLOR)				
86 904237	42828ca	0	panjun	junma_huang@yahoo.co	0	(BLOR)				
87 902229	patimad43	1	lanlan	luc_wang@yahoo.com	0	(BLOR)				Sunday 9th of October 2011
88 909033	ch0ng0ua	0	lijuan	johnmehatituang@rednet	0	(BLOR)				Monday 5th of March 2012 1
89 9070326	etand43	0	Elsen	elzen_cute2009@yahoo.com	0	(BLOR)				

Fig.7. Database on mymu account

Figure 8 presented my.mu.edu.ph website that allows the students to register their individual account in order to view their grades and to update their bill of payment. Then, their account in this website will be used in accessing captive portal. Figure 9 presented the tables of radius database where captive portal looks for its users. Only those who registered the mymu account and passed the turnstile student data will be inserted in this database.

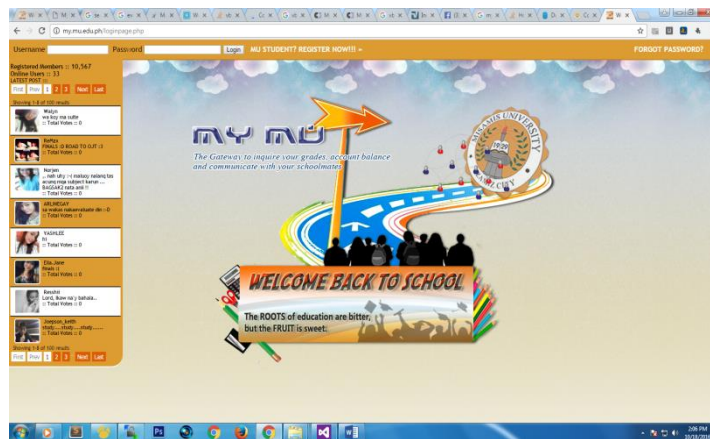


Fig.8. my.mu.edu.ph website

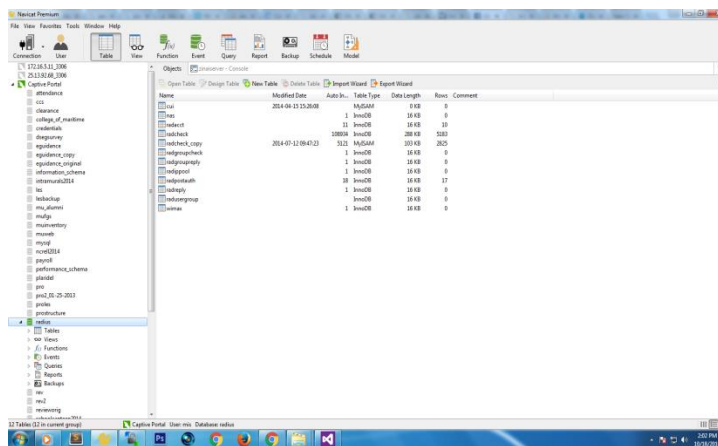


Fig.9. Tables of radius database

Figure 10 presented the username and password of the students who successfully passed the turnstile that will be used as active users in the captive portal. Username contained the student’s id number and password was encrypted. Student should keep their password confidential and not disclose them unless explicitly authorize by the management for retrieval purposes (for example, the student forgot the password).

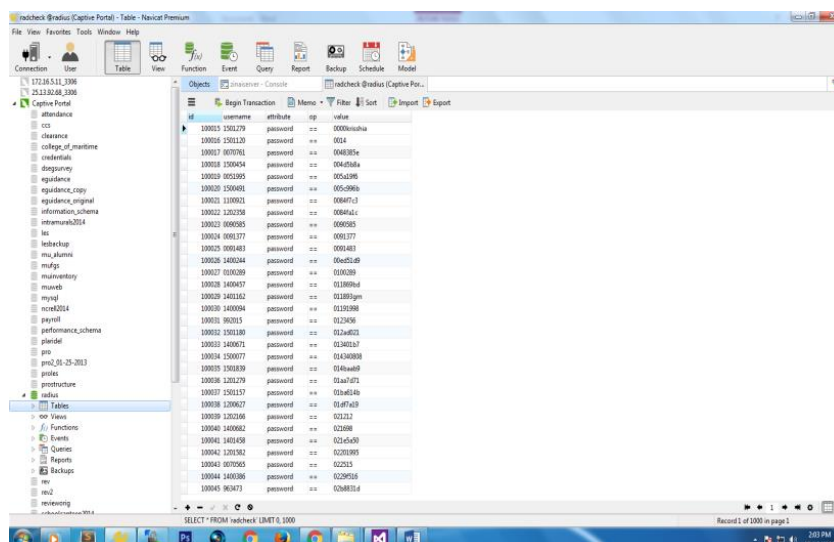


Fig.10. Username and password of students

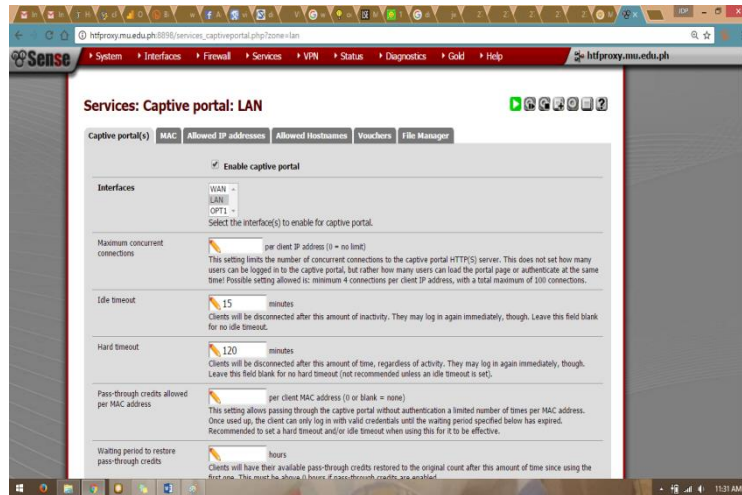


Fig.11. Captive portal configuration

Figure 11 presented the configuration of the captive portal using PFSense. It was applied in the LAN interface. Student will be disconnected after 15 minutes of inactivity and 120 minutes disconnection regardless of activity. If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted. In addition, a popup window will appear when students are allowed through the captive portal. Concurrent user logins is disabled which means only the most recent login per username will be active. Subsequent logins will cause devices previously logged in with the same username to be disconnected. Part also of the configuration is the bandwidth allocation for the internet users. Lastly, the radius authentication is enabled in order to get student's data from mymu server who passed the turnstile and who made mymu account can access the captive portal. Figure 12 presented the feature of PFSense in connecting radius database for the captive portal users.

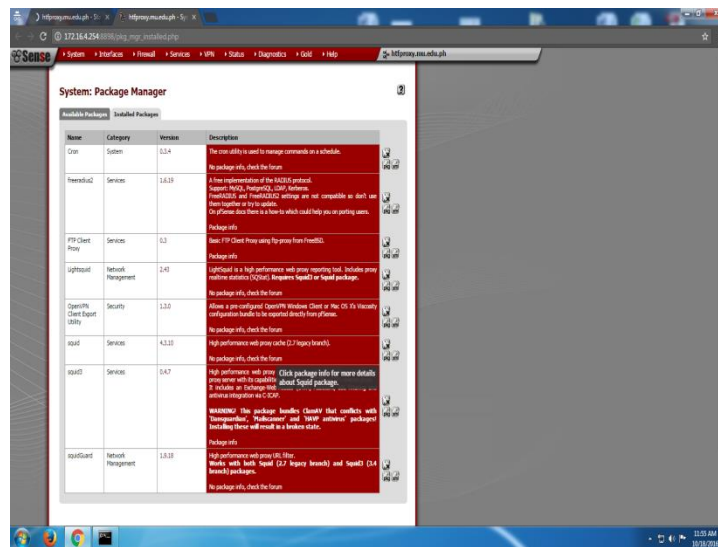


Fig.12. Radius feature

Figure 13 presented the captive portal authentication form that allows the students to access the internet. Only those who are currently enrolled students, who has mymu account and those who pass the turnstile can login the captive portal successfully.

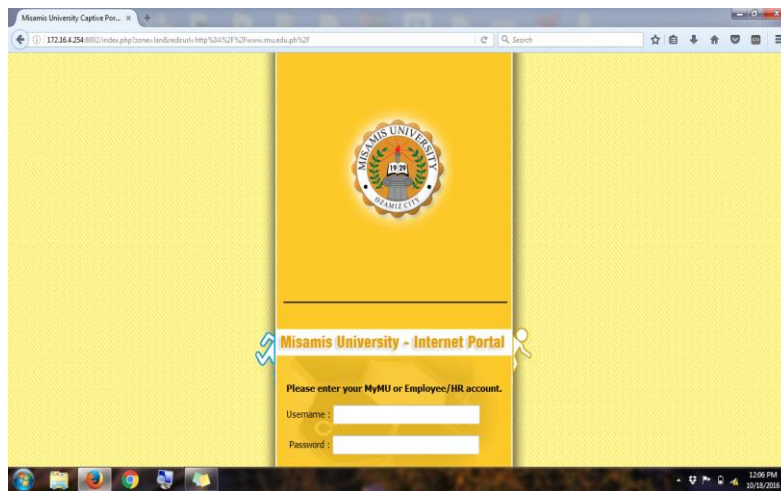


Fig.13. Captive Portal authentication

V. Conclusions and Recommendations

As described in the paper, there is a developed system created by interfacing the turnstile technology to the captive portal of the university. In order to extract data from the turnstile, the researcher used the ZK SDK in which the students' data were imported from the Registrar's database to store the currently enrolled students and to validate also their identification using RF ID. From the turnstile host monitoring, it will send a message to the mymu server in order insert the list of students who pass the turnstile and who had mymu account in the captive portal using radius database. The radius database is a storage of students which will be inserted in the captive portal server for the internet access with the use of the free radius feature of PFSense. PFSense is software that is used to configure the captive portal. The security measure in the study is found by allowing internet access to the students who were currently enrolled, who passed the turnstile and who registered the mymu account. There is a balance of access control and security implementation since the students will only register once using their mymu account in which that account will be used then in the captive portal authentication. Authentication in the captive portal requires the student to input username which is the student's id number and the password. As part of the feature used in the captive portal configuration using PFSense, concurrent logins is disabled which means only one device is required for one account or student user. Deletion of all users in the radius database was done every 5:00 in the morning in order to insert new users who pass the turnstile and who log in the captive portal using the mymu account.

Higher education institutions should utilize the developed system in order to maintain the security of internet access in their respective organization.

For future work, the researcher would like to recommend on the monitoring of students activities conducted in the web as well as identifying the use of internet. Furthermore, it is also recommended in identifying the year level of the internet users and applies user privileges in the internet access.

References

- [1] Cote Parra, G. E. (2015). Engaging foreign language learners in a web 2.0-mediated collaborative learning process. *Profile Issues in Teachers Professional Development*, 17(2), 137-146.

- [2] Wazid, M., Das, A. K., Kumari, S., Li, X., & Wu, F. (2016). Provably secure biometric-based user authentication and key agreement scheme in cloud computing. *Security and Communication Networks*, 9(17), 4103-4119.
- [3] Crane, G. E. (2016). *Leveraging Digital Communications Technology in Higher Education: Exploring URI's Adoption of Google Apps for Education 2015*.
- [4] R. Van, S. Williams, and K. Zirkle. Balancing pedagogy, student readiness and accessibility: A case study in collaborative online course development. *The Internet and Higher Education* 28. 2016. pp. 1-7.
- [5] T. Brabazon. *The University of Google: Education in the (post) information age*. Routledge. 2016.
- [6] Almasi, M., Machumu, H., & Zhu, C. (2017). Internet use among secondary schools students and its effects on their learning. In *Proceedings of INTED2017 Conference 6th-8th March*.
- [7] S. Bashir, K. Mahmood, and F. Shafique. Internet use among university students: a survey in University of the Punjab, Lahore. *Pakistan Journal of Information Management & Libraries (PJIM&L)* 9.1. 2016.
- [8] T. Almarabeh, L. Rajab, and Y. K. Majdalawi. Awareness and Usage of Computer and Internet among Medical Faculties' Students at the University of Jordan. *Journal of Software Engineering and Applications* 9.05. 2016. p.147.
- [9] A. N. Daniel. *Development of a Framework for the Use of E-Learning in Teaching Industrial Technical Education in Nigerian Universities*. Diss. 2016.
- [10] E. M. D. Model. (2016). *Enabling Meaningful Certificates from Massive Open Online Courses (MOOCs)*.
- [11] Zhang, Y., Zheng, D., & Deng, R. H. (2018). Security and privacy in smart health: Efficient policy-hiding attribute-based access control. *IEEE Internet of Things Journal*, 5(3), 2130-2145.
- [12] Ferris, J. M. (2015). U.S. Patent No. 8,984,505. Washington, DC: U.S. Patent and Trademark Office.
- [13] Dominguez, G., Hammill, S. J., & Brillat, A. I. (2015). Toward a usable academic library web site: A case study of tried and tested usability practices. *Journal of Web Librarianship*, 9(2-3), 99-120.
- [14] Smith, S. G., O'Connor, R., Aitken, W., Curtis, L. M., Wolf, M. S., & Goel, M. S. (2015). Disparities in registration and use of an online patient portal among older adults: findings from the LitCog cohort. *Journal of the American Medical Informatics Association*, 22(4), 888-895.
- [15] Chen, Y. H. (2015). Testing the impact of an information literacy course: Undergraduates' perceptions and use of the university libraries' web portal. *Library & Information Science Research*, 37(3), 263-274.
- [16] J. A. Mobarak, C. K. Lang, and O. C. Sen. Proxy captive portal traffic for input-limited devices. U.S. Patent No. 20,160,156,719. 2 Jun. 2016.
- [17] J. P. Gerval, and Y. L. Ru. *Smart Classroom*. *Smart Education and e-Learning 2016*. Springer International Publishing, 2016. pp.415-422.

- [18] H. Liu, and S. G. Tonkin. Apparatus and methods for access solutions to wireless and wired networks. U.S. Patent No. 9,264,435. 16 Feb. 2016.
- [19] P. Bar, et al. Transient mobile application capture in a restricted area. U.S. Patent No. 20,160,014,660. 14 Jan. 2016.
- [20] J. Walz, K. Lowe, and D. Nack. Applying a credit card account on a mobile device. U.S. Patent No. 20,160,155,191. 2 Jun. 2016.
- [21] S. Venkiteswaran and C. A. Calamari. Private wireless communication network for guest users. U.S. Patent No. 20,160,037,338. 4 Feb. 2016.
- [22] S. G. Canning, S. W. Gee, and S. B. Weeden. Confidence-based authentication discovery for an outbound proxy. U.S. Patent No. 20,160,119,327. 28 Apr. 2016.
- [23] S. Scherzer. Method and system for selecting a wireless network. U.S. Patent No. 9,332,486. 3 May 2016.
- [24] B. Nambiar, G. Voon, and R. Verma. System and method for maintaining captive portal user authentication. U.S. Patent No. 9,100,242. 4 Aug. 2015.
- [25] Pinho, C., Franco, M., & Mendes, L. (2018). Web portals as tools to support information management in higher education institutions: A systematic literature review. *International Journal of Information Management*, 41, 80-92.
- [26] Singh, S., Jeong, Y. S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications*, 75, 200-222.
- [27] Downer, K., & Bhattacharya, M. (2015, December). BYOD security: A new business challenge. In 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity) (pp. 1128-1133). IEEE.
- [28] Chaudhry, S. A., Mahmood, K., Naqvi, H., & Khan, M. K. (2015). An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography. *Journal of Medical Systems*, 39(11), 175.
- [29] Vijayarathy, L. R., & Butler, C. W. (2015). Choice of software development methodologies: Do organizational, project, and team characteristics matter?. *IEEE software*, 33(5), 86-94.