WI-FI Internet Browsing Architecture Via BYOD for Smart Campus

Nilaykumar Kiran Sangani, Tejas Vithani, and Nand Kumar

***Abstract*—Smart Campuses are being created throughout all the current industries. Educational campuses, Large organizations, SMEs, Military and Defense are few of the examples of such entities implementing their campuses with the idea of smart computing. Fashioning the campus Wi-Fi enabled is one of the imperative requirements for the campus to be smart. The demand for enabling Internet browsing via Bring Your Own Device (BYOD) using smart and pervasive devices is increasing. With the development of BYOD, the popularity to allow them in campuses has been increased to give a flexible and relaxed policy to the internal manpower and visitors. Implementation of BYOD policy for WI-FI Internet browsing raises a challenge in building a secure browsing experience. In this paper, we aim at building a secure architecture that will segregate the Internet browsing into two zones – Internet Restricted Zone (IRZ) & Internet Public Zone (IPZ).**

***Index Terms*—BYOD, Smart Campuses, WI-FI, Secure Browsing, Pervasive Computing.**

I. Introduction

IN today's world, online connectivity has no boundaries. Smart devices are the commencement of tools to offer on-demand means of online / offline communication [1] [2]. Organizations, Universities, Small and Medium Enterprises, Government entities etc. are moving towards BYOD (bring your own device) policy [3][4]. A smart camp encompasses of pervasive elements, which lead to creation of environments combining computing and communication integrated with human user [5]. Rise in development of wireless technologies and pervasive computing, smart Wi-Fi enabled campuses are built to augment the rich Internet browsing experience for the users [5]. According to a survey conducted by Cisco in 2012 in US, 95% of the participants prefer their staffs brining their own devices for connectivity [6].

In this day and age, external visitors visiting an organizations/university campus would like to connect to the Wi-Fi in order to browse the Internet. Studies have shown about the security problems arising when internal personnel or external visitors connect personal devices to the smart campus infrastructure [6]. There are several advantages for the employees / students / entities and visitors to browse the Internet/ network via BYOD [6]. In a smart campus, the Internet should be available all-around the clock without any constraints. The smart devices and the services should be adept in interconnecting with each other in a diverse milieu.

Pertaining to Confidentiality, Integrity and Availability, there will be always concerns arising such as – Is the device brought by the external visitor, which is connected, to the Wi-Fi, safe and secured? Will it hamper the organization/university's data? When an internal personnel or external visitor attaches a personal smart device into the Wi-Fi enabled network, security becomes a fear [2]. If the Internet and Intranet zones are not segregated accurately, malware from the personal device can be transmitted to the internal organizations/university's network [2]. At the same time, sensitive data can be transferred onto the private device.

In this paper, we propose a secure Internet Restricted Zone and Internet Public Zone Wi-Fi Internet browsing architecture via BYOD, which will succor the smart camps towards the implementation of safe browsing policy.

II. Design

A. Visitors Flow

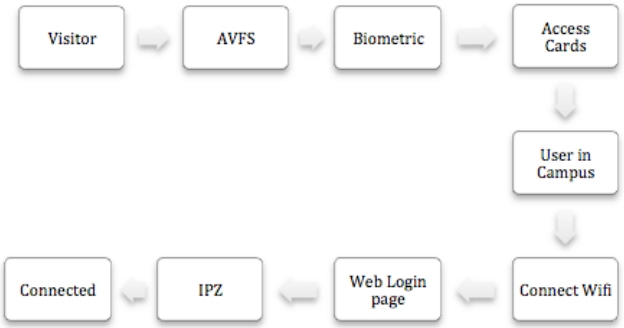

Fig. 1. Visitors Flow

The visitor's flow for accessing the Internet begins with the registration of the visitors at the entrance. The visitor will enter their personal details such as name, date of birth with the help of AVFS (Audio Voice Feeder System). Once entered, the visitors have to register themselves via a biometric system. The data from the biometric system will be delivered to an internal log server for the records. After the completion of the AVFS and Biometric, an access card will be generated having four fields: Username, Password, a

Manuscript received July 23, 2013; revised July 23, 2013.

N.K.K.Sangani is working with Abu Dhabi Company for Onshore Oil Operations (ADCO), Abu Dhabi, U.A.E as an IT Security Planning Analyst. He is also a student with the Computer Science Department, M.E (Software System), Birla Institute of Technology and Science Pilani, Dubai Campus, Dubai, UAE (email: sanganinilay@hotmail.com).

T.Vithani is a student with Computer Science Department M.E (Software System), Birla Institute of Technology and Science Pilani, Dubai Campus, Dubai, U.A.E (email: tejas.vithani@gmail.com).

N.Kumar is Lecturer with the Computer Science Department, Birla Institute of Technology and Science Pilani, Dubai Campus, U.A.E (email: nandkumar@bits-dubai.ac.ae).

random generating token number and expiry date. All of the fields are read only. Now the user has all the required details to connect to the Internet via the smart camps Wi-Fi. The user connects to the Wi-Fi network SSID and receives a Web Login Page in their smart device asking for the following fields: Username, Password and Token. Once the credentials are supplied, the visitor will be routed to an internal guest network called 'Internet Public Zone' (IPZ). IPZ connection will be the country's local Internet Service Provider (ISP), which will be kept in an isolated zone not linking to the campus network. The restriction policy will be of the local ISP.

A. Internal Personnel Flow

Fig. 2. Internal Personnel Flow

The internal personnel flow is distinct when compared to that of the visitors flow as internal personnel are already registered with their username and password. When the internal personnel connects to the Wi-Fi network SSID with their personal smart devices they will be asked to enter the basic login details such as username and password to access the Internet in a web login portal. Once the credentials are supplied, they will be routed to the smart camps internal restricted network called 'Internet Restricted Zone' (IRZ). IRZ is a policy driven controlled environment useable for internal personnel browsing with limited access.

III. UML DESIGN

A. Visitors Sequence Diagram

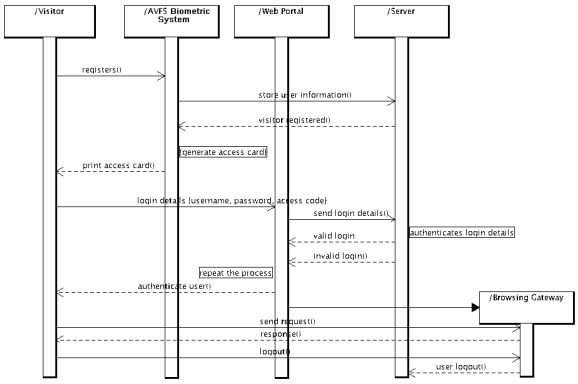

Fig. 3. Visitors Sequence Diagram

Functions in Visitors Sequence Diagram

-Register: The visitor registers themselves at the AVFS and Biometric System.

-Store User Information: The System will store the user information in the server.

-Visitor Registered: The visitor is registered with the campus.

-Print Access Card: The System will print the access card with username, password, a random generating token and expiry date used in web login portal.

-Login Details: The visitor enters the login details provided by the system in the web portal.

-Send Login Details: The web login portal will then validate the users login details.

-Valid Login: If the entered credentials are correct, the user is valid and will be able to access the web.

-Invalid Login: If the entered credentials are incorrect, the user is asked to repeat the login process.

-Authenticate User: The web portal authenticates the users.

-Send Request: The user sends the request i.e. to access the web

-Response: The response to the user request is given via browsing gateway.

-Logout: The user requests for the logout of the session.

-User Logout: The user is logout as requested.

B. Internal Personnel Sequence Diagram

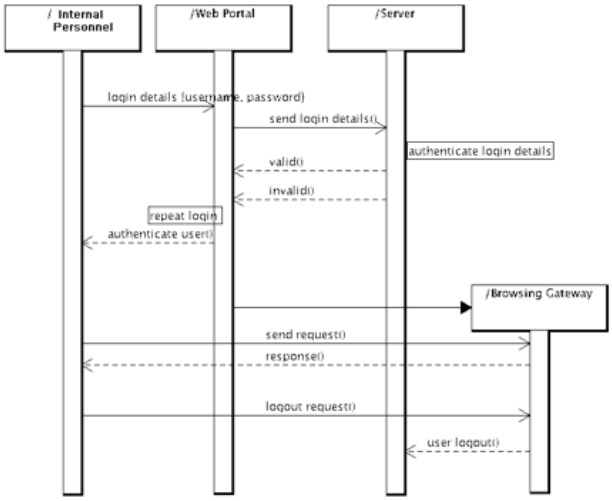

Fig. 4. Internal Personnel Sequence Diagram

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Functions in Internal Personnel Sequence Diagram

-Login Details: The Internal Personnel enters the login details provided by the system in the web portal.

-Send Login Details: The web login portal will then validate the users login details.

-Valid Login: If the entered credentials are correct the user is valid and will be able to access the web.

-Invalid Login: If the entered credentials are incorrect the user is asked to repeat the login process.

-Authenticate User: The web portal authenticates the users.

-Send Request: The user sends request i.e. to access the web.

-Response: The response to the user request is given via browsing gateway.

-Logout Request: The user requests for the logout of the session.

-User Logout: The user is logout as requested.

IV. Identification of Pervasive Elements

Following are the pervasive elements identified for the proposed design architecture:

-Audio Voice Feeder System: This system will take users registration details in the form of voice inputs.

-Biometric System: The user will use this system to register them via fingerprint and face recognition that will be stored in the server logs for identification control.

-Smart Cards: Smart Cards are printed with user's registered details along with their photograph.

-BYOD: Users personal smart devices such as mobile phones, tablets, laptops etc.

-Blade Servers: High configuration servers to run the server OS, Database to store the application logs.

-Wi-Fi Access Point: Offering Internet connectivity.

-IPZ and IRZ servers: IPZ and IRZ servers separated within the network.

V. Conclusion

This paper proposes a secure Wi-Fi Internet browsing architecture via BYOD, which will safeguard the campus web-browsing network by separating the connectivity through IPZ & IRZ, also protecting Wi-Fi web login authentication security with the usage of smart cards having expiry tokens instrumenting two-factor authentication.

VI. Future Work

Future work will include the detailed component policy implementation standards of the Internet Public Zone, Internet Restricted Zone services and the comprehensive specification of the pervasive elements for the execution of the proposed architecture.

References

[1] Lennon, R.G., "Changing user attitudes to security in bring your own device (BYOD) & the cloud," Tier 2 Federation Grid, Cloud & High Performance Computing Science (RO-LCG), 2012 5th Romania, vol., no., pp.49,52, 25-27 Oct. 2012

[2] Miller, K.W.; Voas, J.; Hurlburt, G.F., "BYOD: Security and Privacy Considerations," IT Professional, vol.14, no.5, pp.53,55, Sept.-Oct. 2012

[3] "A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs", August 23, 2012, http://www.whitehouse.gov/digitalgov/bring-your-own-device

[4] Sangani, N.K.; Vithani, T.; Velmurugan, P.; Madiajagan, M., "Security & Privacy Architecture as a service for Small and Medium Enterprises," Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on , vol., no., pp.16,21, 8-10 Dec. 2012

[5] Satyanarayanan, M., "Pervasive computing: vision and challenges," Personal Communications, IEEE , vol.8, no.4, pp.10,17, Aug 2001

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)