International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 10 61 - 64

Access Constraint Of Intelligent System Over Wi-Fi Network - A Propose Plan

Gayatri Lokhande
Computer Sci. & Engineering
Nagpur Institute of Technology
Nagpur, India
glokhande272@gmail.com

Pradeepti Shrivastava
Computer Sci. & Engineering
Nagpur Institute of Technology
Nagpur, India
pradeepti629@gmail.com

Shefali Tajne
Computer Sci. & Engineering
Nagpur Institute of Technology
Nagpur, India
shefali.tajne1994@gmail.com

Bhagyashri Tijare
Computer Sci. & Engineering
Nagpur Institute of Technology
Nagpur, India
btijare1@gmail.com

Snehal Ambulkar
Assisstant Proffessor
Computer Sci. & Engineering
Nagpur Institute of Technology
Nagpur, India
ambulkar.snehal2290@gmail.com

bstract- The growing ubiquity of public wireless network in university campus, corporate sector and other settings. The logical separation of user permission and security has become a matter of concern. To solve this problem, dual layer authentication is introduced in term of One Time Password (OTP) which is difficult to guess and not easily hacked or cracked by user. The concepts of time constraint mechanism for access control to limit the network usage and bandwidth utilization. Time constraint is different depending on the type of user. Another feature of this proposed paper is connection termination when system is idle for certain period of time.

Keywords - *One time password, Time constraints, access constraint, connection termination.*

*****

I. INTRODUCTION

The expansion of wireless network in homes, corporate offices, university campuses and public hotspot mirrors vigorous growth of wireless network in the consumer and worldwide. Security and access constraint over internet based services is always a challenging issue i.e. to provide admission control, user permission and management It is always a challenge due to increase in market and utility compromised the security issues such as data tampering, password hacking and many more. The Wi-Fi system uses four methods for controlling the access i.e. Open System Authentication, Pre shared key, user name, password and MAC address whitelisting/ blacklisting. The problem with these mechanisms is that, it gives rise to a number of potential attacks, both passive and active. Due to absence of access constraint during working hour, which leads to Service violations (i.e. Exceed in number of connections permitted by internet service provider), Bandwidth shortages (i.e. Users piggybacking on your internet connection might use up your bandwidth and slow your connection) and slowdown connection

Now a days two factor authentication is used in terms of one time password. The generation and transmission of OTP is also a serious issue, some organization used mail facility and some used mobile devices. The mobile device used SMS facility for receiving an OTP password the interpolation derivative with MD5 hash algorithm is used for OTP generation. This paper aims to provide access constraint and time constraint to limit the access of Wi-Fi services depending on the discrete time representation and periodic time representation. Automatic connection termination mechanism is proposed when client remains inactive for 15 minutes after connection termination. In section 2 discuss the literature review. In section 3 discuss the proposed plan. In section 4 discuss the methodology and finally discuss conclusion and future scope in section 4.

II. RELATED WORK

In [1], authors propose an OTP based cloud access control model for enhancing security. They used AES encryption interpolation derivatives and MD5 hash algorithm for processing mathematical operation. These algorithm aims to reduce time required for OTP generation, verification and validation of this algorithm is performed on Cain and Abel tool. Where it cannot be hacked or cracked.

In [2], a fast authentication scheme is proposed to improve handoff performance for WiFi network (handoff is a process of switching access points). A novel MAC layer authentication scheme that uses tunnel technology to minimize authentication latency and provide secure communication

In [3], author describes a new approach that is, four tuple representation of time combined with discrete time representation and periodic time representation. They derived

function and algorithm for computation of state change of time and conflicts detection and resolution based on XACML (Extensible Access Control Markup Language) and entities overlapping detection.

In [4], authors introduced TDMA/FDD based MAC protocol for wireless data communication, providing QoS guaranteed for real time multimedia application and detailed CBP analysis of different service classes. The simulation model of the proposed MAC scheme is realized using OPNET modeler network simulator.

In [5], portray method of implementing two factor authentications on mobile phones by providing one time password mechanism to enhance the security level. Several factors are considered in OTP algorithm in order to generate difficult-to-guess password. The factor which are chosen in this algorithm are IMEI number, IMSI number in user name, Hour, minute, day, year/months/date.

In [6], a dual timers and termination of connection mechanism implemented when preset period of inactivity is detected, user connectivity to network is automatically terminated. Three-way handshake procedure is used by timer 1 and timer 2 to terminate the connection after a preset period of few seconds.

III. PROPOSED SYSTEM

The proposed paper, emphasis to provide a secure network that properly manages Access, Confidentiality, and Authentication, Integrity, and Non- repudiation in educational organization. Authorized user can access the network through predefined channel whose ID is stored in organization database. When the user tries to access the Wi-Fi service, they will be redirected to Login link. The systems uses dual authentication in terms of One Time Password which is to be sent on registered Mobile number. The OTP increase the security strength of access control over Wi-Fi network. The main objective of proposed system is to provide time constraint to limit the access of Wi-Fi services depending on the type of user and schedules of working hours and to provide automatic connection deactivation mechanism when user is remain inactive for 15 minutes after connected to Wi-fi.

Types of User:

The proposed system works on four types of user depending on schedule of working hours.

1. System Administrator:

   The system administrator monitors, maintain and update the records in the database. Role of admin is to add newly admitted students and recruited employees and to remove them, when students or employees leave the institute. When workshop or some other programs are scheduled in college, event updation is done by admin in data base to provide special privilege to the guest user. System administrator can monitor monthly report of usage of the WiFi services.

2. Employee:

   Authentication is provided using registered mobile number employee id when registering on the system of organization. While login process OTP sent on registered mobile number.

   There are three key types of employees-

   a. Teaching staff: The duration of Wi-Fi service for teaching staff is of 2 hours. The teaching staff has authority to provide special privilege to add guest for workshop according to the events updated and also have privilege to block student access and view records of students if any.
   b. Non-teaching staff: The duration of Wi-Fi service for non-teaching staff is of 2 hour. There will not be any kind of special privilege.
   c. Administrative staff / Clerical staff: Administrative staff has 2 hour connectivity for Wi-Fi service to provide special privilege to add guest for workshop when event is updated in the database.

3. Student:

   The student is authenticated via registered mobile number when login on the system and further, OTP sent on registered mobile number. Student can access the Wi-Fi service during free hours (i.e. Recess time) which is associated with scheduled time table. If student tries to access the Wi-fi for more during lecture hour then a report will be generated and forwarded to class In-charge.

4. Guest User:

   If guest or unauthorized user tries to access the network via Login link using mobile number , the system check for special privilege from employee (teaching staff and administrative staff only) for the mobile number entered by the guest. If entry is valid according to Updated Event in the database guest can access the Wi-fi for specified time duration (i.e, 2 hours), else the Access is restricted by the system (i.e. ACCESS DENIED).

Functionality of the proposed system is as shown in the flow chart (Figure 1). Figure shows the details of the facilities provide to the type of user and the restriction applied to them.

IV. METHODOLOGY

In this section, we discuss the algorithm of OTP generation using the interpolation derivatives and MD5 hash algorithm. Time constraint mechanism and connection termination when is user is inactive.

 ISSN: 2321-8169
61 - 64

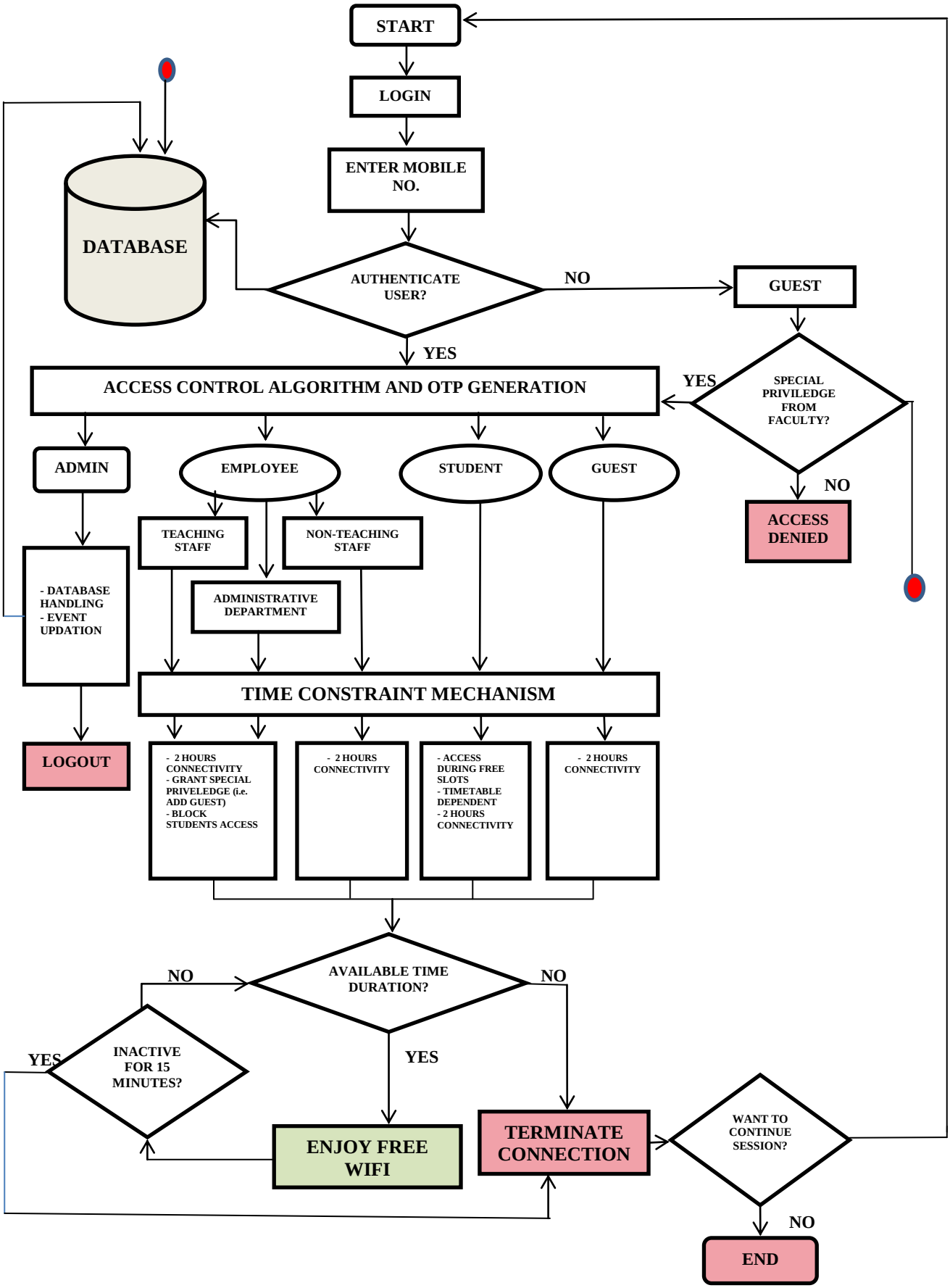

Figure1. Flow Chart of Proposed system

A. OTP GENERATION:

OTP generation uses the interpolation derivatives and MD5 hash algorithm. The interpolations derivate derived the input massage in terms of mobile number and create a variable size matrix for the processing of input data of hash algorithm and randomly select the 6 bit data for OTP transmission. Algorithm of Access constraints mechanism is applied during the time of OTP generation. When user enters their mobile number for login, then on the basis it, "types of user" is determined from database and according to it access constraints is will be applied.

B. TIME CONSTRAINT MECHANISM:

Its main motive is to restrict the user from access uses of WiFi during working hour and limit the speed distribution if users are idle. Time constraint mechanism is used in proposed system to limit the access of users over Wi-fi and further connection will be terminate, if user is inactive for 15 minutes during connected with Wi-fi. In proposed system, depending on the type of users time restriction is applied. No user will be allowed to access the wifi after the allotted time limit.

C. CONNECTION TERMINATION ON INACTIVITY:

Using timers and logs concept, if client is inactive for 15 minutes, connection will be automatically terminated, Similar to the concept of Keep-alive timer. Whenever server hears from client, it resets keep-alive timer. If server does not hear from client, it sends a probe segment. If there is no response, it assumes that the client is down and terminates the connection.

V. CONCLUSION

In this proposed paper, we offered a method for enhancing the wireless network security and limit the over usage of Wi-Fi during working hour in an organization. The Access constraint mechanism allows authorized user to access network using secondary level authentication scheme in terms of one time password (OTP). Time constraint algorithm provides access depending on user's type. This eventually helps in reducing network traffic and proper bandwidth distribution of Wi-Fi network. OTP generation algorithm takes minimum key generation time from other OTP generation algorithm and reduces the security risk over Wi-Fi services. Additional functionality is Three-way handshaking procedure which terminates the connection when user remains idle for 15 minutes after connected to Wi-Fi.

VI. FUTURE SCOPE

In future, advanced algorithms can be used to develop more reliable and secured system for time constraint to control access and provide advanced mechanism for OTP generation

ACKNOWLEDGEMENT

This research paper is made possible with the help and support of our parents, teachers, family, friends, and all the people who guided us throughout our work. Especially, we would like to thank all the other professors of my department who have suggested and helped us in writing this paper. Finally, we sincerely thank to our parents, family, and friends, who gave us emotional and financial support. Without the support of these people the product of this proposed paper would not be possible.

REFERENCES

[1] Priyanka Patel and Nirmal Gaud, "Access Control for Cloud Computing Through Secure OTP Logging as Services", International Journal of Computer Applications (0975–8887) Volume 141– No.14, May 2016.

[2] Zhenxia Zhang, Richard W. Pazzi and Azzedine Boukerche, "Design and Evaluation of a Fast Authentication Scheme for Wi-Fi-based Wireless Networks", June 2010.

[3] Chunyan Han, Lianzhong Liu, Yifei Yuan, "Time constraints of Access control", Transtech Publication, Switzerland, August 2014.

[4] Sedat Atmaca, Alper Karahan, Celal Ceken, Ismail Erturk, "A new MAC protocol for broadband wireless communications and its performance evaluation", Faculty of Engineering, Computer Engineering Department, Turgut Ozal University, 06010 Ankara, Turkey, 25 July 2013.

[5] Wassim El-Hajj, Fadi Aloul, Syed Zahidi, "Two Factor Authentication Using Mobile Phones", IEEE 2009.

[6] Nygil Alex Vadakkan, S.E.Vinodh Ewards, "Detection of Denial of Service by Access Pattern Assessment", 2014 International Conference on Electronics and Communication Systems (lCECS-2014), Feb.13 -14, 2014, Coimbatore, INDIA.