IJCAT - International Journal of Computing and Technology, Volume 3, Issue 6, June 2016
ISSN : 2348 - 6090
www.IJCAT.org

System Security Using Bluetooth with Remote Access

[1] D.S. Adane, [2] Anuja Fole, [3] Megha Rajput, [4] Ajay Kabra, [5] Anurag Tomar

[1,2,3,4,5] Department of Information Technology,
ShriRamdeobaba College of Engineering and Management,
Nagpur, India

Abstract - The traditional authentication mechanism used for a standalone or shared system is through Alphanumeric or Graphical passwords. Typical threats to passwords include Guessing, Offline Dictionary attacks, Spoofing, Shoulder Surfing and Social engineering or pretexting. Even when the Graphical passwords are used the accuracy, computational and storage overheads prohibit the use of this type of passwords, especially for low cost end user systems. We propose a technique, using Bluetooth technology on smart phones, to not only authenticate the user on a shared system, but also ensure that his / her data is safe (in encrypted form) when he / she is not accessing it. The data gets automatically decrypted when the user is within the range of the system. Another novel feature includes remote notification on system access when the user is outside the range (not in the vicinity) of the system. This feature enables the user to have total control of the system, as the user is made aware of the system access in his or her absence. We think this feature is extremely relevant for shared as well as unshared system holding sensitive data. Thus, the proposed work provides Authentication, Data Confidentiality and Remote access notification to the user working on a shared or unshared system.

Keywords **- Authentication, Confidentiality, Bluetooth, Remote Access, Encryption, Security, Shared System.**

1. Introduction

Today in the information age, computer has become an integral part of every body's life. Systems mobility feature has expanded the usage of computers accompanying the user wherever he goes. Most of the corporate people and students use system frequently. It is used for many purposes like running various applications, software's and most importantly storing personal data, personnel data, project data or sometimes even confidential data. Even though recent operating systems have come up with decent security features most of them can be bypassed to get access to stored information. The cheapest and most common used method of computer authentication is the use of usernames and passwords. Alphanumeric passwords are used to protect both low and high sensitive information even though several major problems with alphanumeric passwords have been identified. The human capacity for information processing is limited. As a consequence, users are having problems remembering their passwords and more importantly, to memorize and correctly match numerous passwords.This causes users to either use an easy password, which is easy to remember, but also easy to guess or crack, or to use complicated passwords that are hard to guess or compromise but are difficult to remember. Users can use several work-around to overcome their limitations using the same password for every system they access, writing down passwords, storing passwords in electronic files, and reusing or recycling old passwords. The data contained within the organizations are supposed to be sensitiveand there is a need for it to be kept secured.

In this process, organizations tend to impose stringent password policies. However, overall these policies are deemed as user unfriendly by those on whom these policies are imposed. As a user it is very painful to follow this policy and expect to remember the password every time. When users cannot cope up with the demands of strict password policies, it reduces their productivity and leads them to adopt coping strategies which usually reduce security. Also folder protection techniques require passwords for encryption and locking.

The length of passwords plays an important role in determining its strength. Different type of attacks on alphanumeric passwords such as Guessing, Offline Dictionary attacks, Spoofing, Shoulder Surfing and Social engineering or pretexting suggests that a different and lightweight approach is required to solve the problem. Even when the Graphical passwords are used the issues of Remembrance, Computational and Storage overheads prohibits the use of this type of password, especially for low cost end user systems.

We proposea novel method foruser authentication, on the personal or shared system, which initiates just when the system starts. The Bluetooth enabled device is used for encryption and decryption in the system. To start with, the user has to register on the system. An administrator can register the users working on a shared system. Whenever aBluetooth enabled smartphone of a registered user goes out of the systems vicinity (range), the personal user folder(s) is (are)encrypted. Similarly, when the smartphone comes in the vicinity (range) of the system, thefolder(s)is (are)automatically decrypted. Our Android app allows sending commands to shut down the system and allow or deny the user accessto system and also getshis snapshot.

2. Work Flow

The figure 1 shows the work flow of our system. When user tries to operate the system, he has to enter the operating system password (if set by administrator) then the screen opens in the form of system application. There are two options, one for registration and other for login. If the user is new to the system then he/she has to register on the system. Among other things, the mobile device details are stored for identification purpose. If the user is not new, then Bluetooth authentication (login) phase gets activated automatically. The new user request goes to the server and from there it goes to mobile application. The mobile application tells the user whether the request was granted or rejected. All the legitimate user device entries are stored in a database. These Bluetooth devices entries are checked in the database to authenticate the user. If the entry is found then the user's folder path corresponding to the address is retrieved from the database and folder is decrypted, otherwise folders remain in encrypted format.

The mobile application is also used for accessing the systemremotely. The following sections give details of implementation of our work.

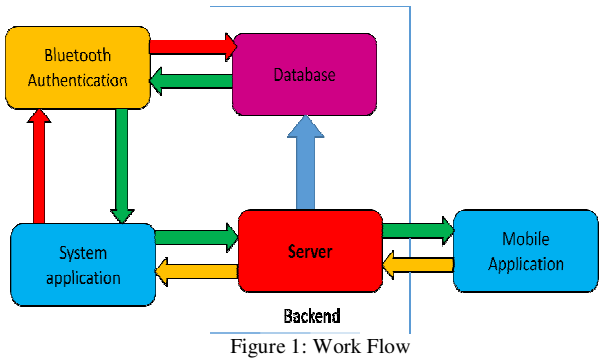


Figure 1: Work Flow

3. Implementation Details

Our work is mainly composed of five components: Bluetooth Authentication, System Application, Sever-Side Application, Mobile Application and Database. They all have an important role in providing strong security against unauthorized access. In this section we discuss each of them.

3.1 Bluetooth Authentication

Authentication is a process that ensures and confirms theuser's identity [1] [2][3] [4].We have used Bluetooth for this purpose [5]. Specifically, we have used Bluecove Library [9], which helps us in searching the devices that are in the range of system's Bluetooth communication. A background process running on the system continuously keeps track of devices within the range. After locating all the devices within the range, it then checks to verify the authenticity of the user w.r.t the system to see if he / she is a legitimate userregistered for the system. Figure 2is a snapshot of how this process works. Every single device in the vicinity of the system is located and authenticated, by the name and address, by the system. Each Bluetooth address is checked with the addresses store in databases and has status as active. If the address matches, then its corresponding encrypted folder changes to decrypted state. A new user needs to register itself and provide necessary details regarding its folder and if the request is approved

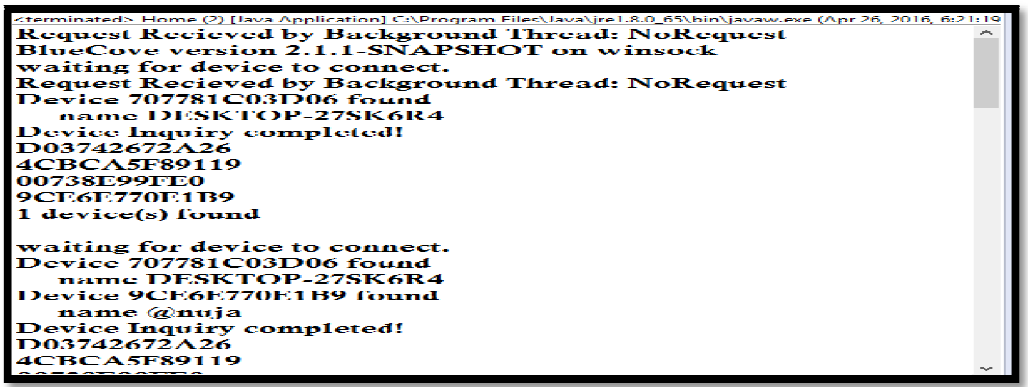


Figure 2: Name and Bluetooth address of searched devices

by system's owner only then the requesting user becomes the authenticate user of the particular system. User details will then be stored in database and is compared if its Bluetooth is in range. If multiple registered users have their devices inrange then access is provided in first-cum-first-serve basis. If a user in not registered but if his Bluetooth isrange, he can donothing with others folder as they will be inencrypted format.This is because a user's folder will be decrypted with their respective Bluetoothaddress (only if it is inrange)only and no one else. A user needs to go through the above procedure to authenticateitself beforeaccessing the information. We have used the AES algorithm [5] [6] [7] [8] for Encryption and Decryption.

After completing successful Bluetooth authentication process, the folder is decrypted by applying the key and algorithm in reverse order. The key used here is 128 bit key. This key is generated using 4 characters and Bluetooth address of user who has successfully passed the authentication test. So this key is unique for every user. Decryption function takes folder path and Bluetooth address as parameter and recursively decrypt the files present in the folder. Similarly, if the authenticated user goes out of range then this same algorithm runs using the same key and Bluetooth address. Encryption function also recursively encrypt each file in that folder. Since the encrypted file is present on the system itself, in order to protect that file we have used icacls command to deny the access of folder to all users. The figure 3 shows the encrypted file.

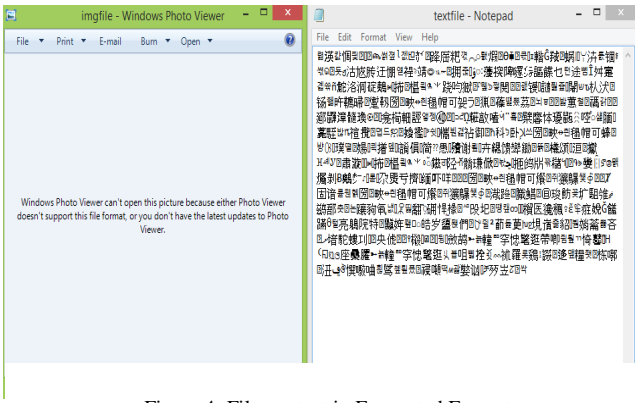


Figure 4: File content in Encrypted Format

3.2 System Application

This application is essentially a user interface. It has two buttons: Login and Register. Register button is used for registering new user. If a user clicks it then he/she is redirected to a request form, which he can fill and send to server if he wants to access the system.Figure 4 shows the user registration form. Login button is for those users who have already registered. Once the button is clicked all the processes start in background right from Bluetooth authentication to mobile application. After this,a background thread runs which continuously checks the request from server-side application which in turn gets that request from mobile application. After getting the request then that particular requested operation is performed on the system. With the help of this mechanism we can even capture user images and send to server. All the components help each other in getting the input from user to processthe inputs and perform necessary operations to give the output. This is the main component on which other components are dependent. The figure 4 shows the register form.

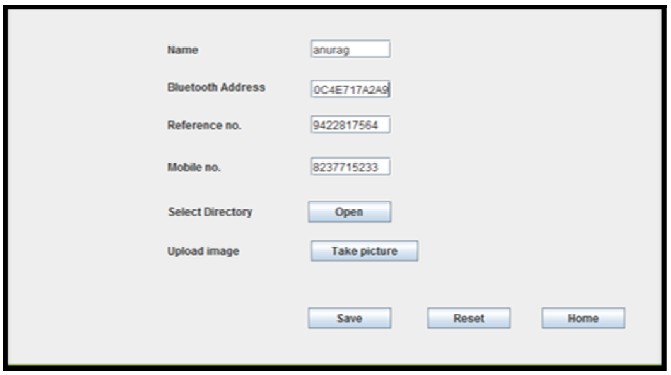


Figure 3: Registration form

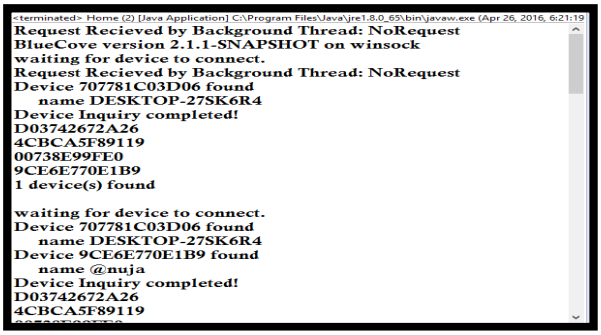
3.3 Server-Side Application

We have used a free hosting server which is created using Hostinger website. This is the mediator between system and mobile application (described in next section).Whatever operation user wants to perform on system using mobile application,the request first goes to server and from there reaches the system. Even if the system application is not on, the request remains on the server itself. As soon as the system application is on, the variable in the background thread reads the particular input from the server and performs a particular action on the system. Similarly, the new user request or the current user details goes from the system to server and then to mobile application. This is the backbone of the system without which remote access functionality would not have been possible.Figure5 shows the complete interaction between the laptop, server and mobile.

3.4 The Mobile Application

Mobile Application is designed to remotely access the system. The owner (Administrator) can completely control

the access to system according to the current user who is willing to access it. He can pass shutdown, recording (till user specific time period) and screen snapshot request to system via server.



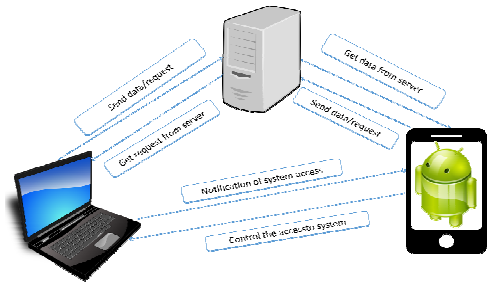


Figure 5: Communication between computer, server and mobile

Figure 6 and Figure 7 shows options available after login screen and the control system application respectively with the menu of options available on each. The owner (Administrator) allows only those people to access the system whose request has been granted earlier or based on the trust level of the user. The owner is also notified about the user who has been currently authenticated by the system to check if the user is the correct user or not.

The user's image and the details corresponding to the identified Bluetooth address are sent to the owner for cross-checking. Owner can also accept the new request and make the user's status as active. He can also delete the new request or even delete the active user if some abnormal activities are detected. Figure 8 and Figure 9 shows the manage user information and edit user information, respectively. The user can control the system by application like shut down the system, get the snapshot of the system, recording of the activities on the system.

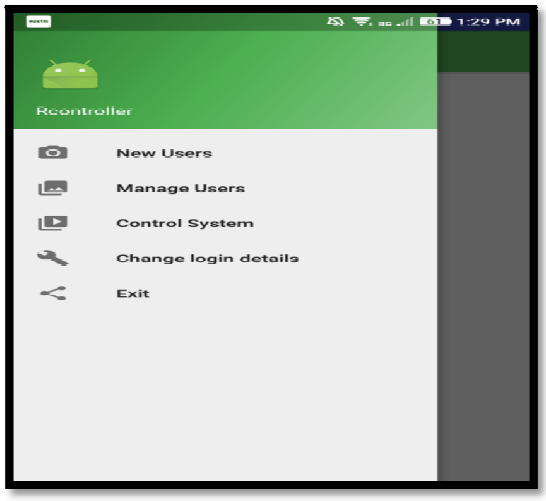


Figure 6:Login Screen details

Figure 7: Control System Application

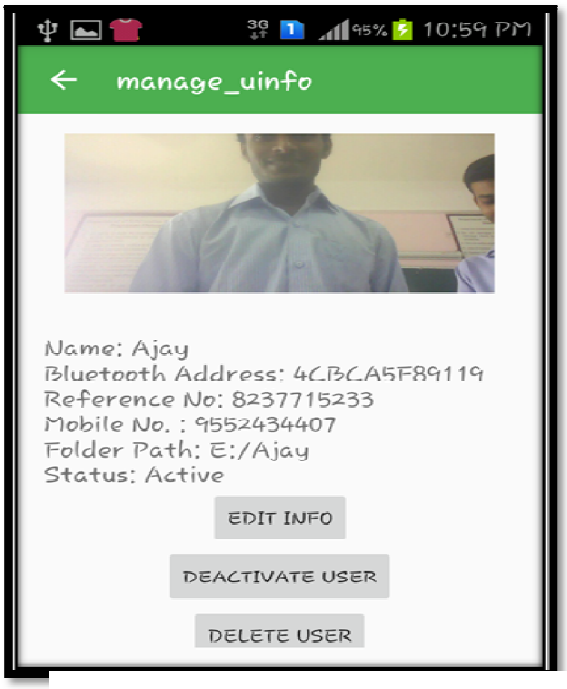


Figure 8: Manage user Information

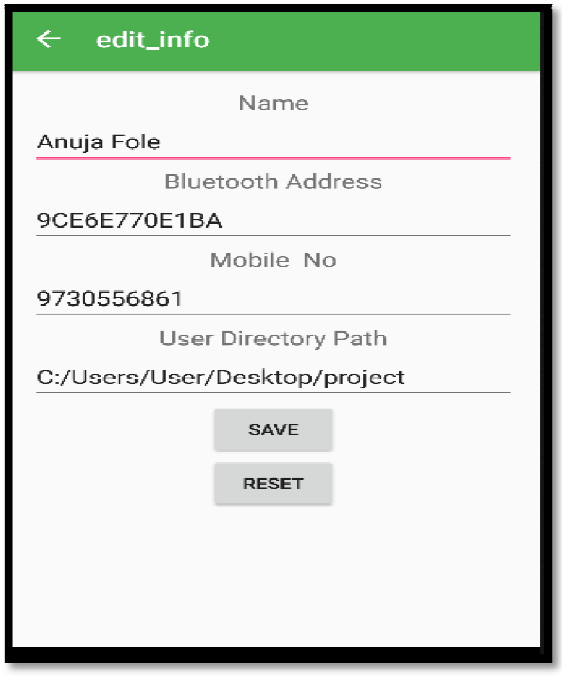


Figure 9: Edit user information

3.5 Database

We have used MySQL to create database on system as well as on server. The database of the system is always updated with server database before the searching for the devices takes place, as the server database is most frequently updated by the mobile application. The database contains the username, Bluetooth address, mobile number, reference number, status, user image and path of the folder to be encrypted. This is also an important component as every time the nearby Bluetooth addresses are compared with the data present in the database. The new entry of the accepted request is also reflected in the database which can be used for comparison, the next time the new user wants to log into the system.

4. Conclusion and Future Work

The text based passwords are always vulnerable to brute-force attack, Dictionary attack, and key loggers. Our proposed solution doesn't use text password for authentication, rather our system uses Bluetooth address of users to authenticate them thus,eliminating all the attacks discussed above. To ensure that two legimate users don't have access to each others directories or files, we are using Bluetooth addresses as the key for encryption thus directory contents of one user can't be decrypted by any other user's Bluetooth address. Systems which are shared between users of organization or family members at home need more security than personal systems, hence, using Bluetooth authentication alone isn't sufficient thus our solution include remote administration application for owner or administrator who can control the remote system via android application that we have designed. Our system is ideal for environment where there is need of system which allows multiple user to store and retrieve data securely. The existing system can be extended by addingfunctionality like Remote Desktop sharing, file transfer and optimization of system.

The current system is developed by considering the need of multiuser and secure environment for users to save their personal data so there is no immediate need of remote desktop sharing for now but we can provide an application for registered users of the system to use the shared system remotely. Each user will have an application installed in their android mobile or other system, with this application users will be able to get the exact image of the remote system and whatever operations performed in the application will be reflected at the remote system. Users will be able to transfer files and folder between remote system and the application.

The existing system transfers request via a middle server and every request transferred is first stored at server and then to the R-controller application hence, there is some seconds of delay for transfer of commands. Registration request and other commands which include image data in the request takes more time to transfer form shared system to server and from server to the application installed on administrators mobile. To reduce this command transfer delay the image data need to be compressed before transferring it to server. Because, if remote desktop sharing functionality is added to the system, then these delays will make the application unreliable.

References

[1] Mrs.ArunaGawde, SanchitJaina ,MohsinMasanib, SahilDeliwala"Securing Computer Device Using Bluetooth technology and One-Time Password",International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 4 April 2015, Page No. 11426-11429.

[2] A.V.Nadargi, ApurvaDalmiya, SonaliJadhav, Gajendra Singh Solanki, "Study of Securing Computer Folders with Bluetooth", International Advanced Research Journal in Science, Engineering and Technology,Vol. 2, Issue 2, February 2015.

[3] NikitaSaple, DhanrajPoojari ,AnkitaKesarkar and AlkaSrivastava , "Securing Computer Folders using Bluetooth and RijndaelEncryption", International Journal of Current Engineering and Technology, Vol.5, No.1 (Feb 2015)

[4] Wankhade S.B., Damani A.G., Desai S.J., KhanapureA.V."An Innovative Approach to File Security Using Bluetooth International Journal of Scientific Engineering and Technology Volume No.2, Issue No.5, PP: 417-423, 1 May 2013.

[5] Nishant Mishra, Vishal. Gupta."An overview of bluetooth security: issues and challenges", Journal of Global Research in Computer Science, Volume 3, No. 3, March 2012.

[6] DhanrajPoojari, AnkitaKesarkar, Nikita Saple and AlkaSrivastava. "Improving Security for Folders in Windows by using Bluetooth and Rijndael Encryption", International Journal of Current Engineering and Technology, Vol.5, No.2 (April 2015)

[7] S. Pavithra and Mrs. E. Ramadevi."Performance evaluation of symmetric algorithms",Journal of Global Research in Computer Science, Volume 3, No. 8, August 2012.

[8] www.aesencryption.net

[9] www.bluecove.org/bluecove/apidocs/overview-summary.html#Device Discovery