BYOD DATA SECURITY IN MOBILE COMPUTING

Divya PremChandran[1], Vrushali Jadhav[2]

[1]Assistant Professor Department of MCA, Bharti Vidyapeeths Institute of Management Information Technology, C.B.D. Belapur, Navi Mumbai, India

[2]Department of MCA, Bharti Vidyapeeths Institute of Management Information Technology, C.B.D. Belapur, Navi Mumbai, India

ABSTRACT

BYOD or Bring Your Own Device has become one of the most popular technology for enterprises/organization to provide mobility and flexibility in workplaces. The emergence of new technologies and features of mobile devices makes them essential parts of every aspect of day to day business activities. Also, mobile networks are now well integrated with the Internet, therefore, in BYOD, the personal devices (i.e. mobile devices) can be used to increase employees satisfaction or they work more efficiently and it also reduces an organization's device costs. Mobile devices are not well protected compared to computer and computer networks and users pay less attention to security. Since as far study of BOYD, security in mobile computing that there are some issues related to private/organizational data are not protected. Therefore in this paper, we help to give an idea that secure data from unauthorized access and theft of data. It is our hope that this review will provide a theoretical background idea for future research and enable researchers to identify more security ideas for Data Security and focused upon how this 3 Level security can be more secured for the user. So 3 Level security provides multi factor facility in authentication to the users.

Keywords : BYOD, 3Level Security, Authentication.

I. INTRODUCTION

BYOD (Bring Your Own Device) is an incipient trend whose principle is to allow employees to utilize their personal devices (like laptops, smartphones) in a workplace. The highlight of BYOD is to ascertain maximum flexibility to increment the productivity of employees and they are more acclimated with mobile devices.

According to Weeger, Wang, & Geewald (2016) Some research indicates that allowing personal mobile devices and smartphones use can accrue benefits to the employer, including increased productivity. In French, Guo, and Shim (2014) research that 80% of users who utilize their own contrivances feel they are being more productive, and found a flexible and accommodating BYOD policy increases overall employee morale. Their research

further suggests BYOD has the potential to preserve the organization money, as the utilizer rather than the organization shoulders the cost of the contrivances, including purchase price and monthly charges, hardware and software purchase charges.

People want a balance between their personal and professional lives. Another Cisco study research workers feel more balance in their professional and personal lives when they're allowed to bring their own devices into the workplace. According to IBM, more than 80% of workers feel Smartphone's will become an

integral part of the workplace in the near future. Businesses already are becoming increasingly creative in their approaches to improving workplace satisfaction and productivity. And BYOD represents an expedient to avail workers feel more balanced while embracing a technology that's already widely utilized.

BYOD increases the speed of work as well as employee satisfaction because of good communication, flexibility of work and fast respond of employee. But then again, the real concern about dealing with BYOD devices and provide the flexibility to access the network with the security at the same time. That's because different threats can appear through allowing BYOD such as losing the Smartphone's, laptop will cause to loss the data in it and it also allow unauthorized users to read data or access that data for their use. Also, damage the devices, worms and harm application which cannot control by the administrator.

To protect any device and system authentication must be provided. There are a many of different authentication methods that can be used to confirm the identity of an authorized person to handle the device and system and data related to that system securely. Previously there are many authentication techniques were introduced such as graphical password, text password, Biometric authentication, etc. generally there are four types of authentication techniques are available such as:

1. Knowledge-based: means what you know. The textual password is the best example of this authentication scheme.
2. Token-based: means what you have. This includes Credit cards, ATM cards, etc as an example.
3. Biometrics: means what you are. Includes Thumb impression, etc.
4. Recognition Based: means what you recognize. Includes graphical password, iris recognition, face recognition etc.

II. OBJECTIVE OF THE STUDY

The proposed 3 Level authentication system is the mixture of various other authentication techniques. In our authentication process we are use Bio-metrics in last level because it is more precise and specific to the authenticated person, there is a total information provided of who is logging in to the system and server side admin, with the finger print and scanner we have managed to store the information to the database ,so it helps to authenticate the concern person.

The Objectives are:
1) To provide secured authentication technique.
2) The system should be more user friendly, easy to use for the user.
3) The system should allow user to select multi password by providing 3levels of security.
4) The system should overcome the limitations of previously made authentication techniques, that can help to secure the data from unauthorized person.

III. LITERATURE REVIEW

Bring Your Own Device (BYOD) (Giddens & Tripp, 2014). According to (Kerr & Koch, 2014, p. 169) Widely embraced by users, corporate IT departments found themselves forced to embrace BYOD to avoid users creating their own unapproved workarounds, referred to as "feral information systems".

According to (French, Guo, & Shim, 2014), As far back as 2013, 71% of organizations had changed they allow the use of personal devices (mobile, Smartphone's) on corporate networks, and 68% of employees were already using personal mobile devices of all types for work.

Research conducted by Markets and Markets predicts that the adoption rate of BYOD policies among North American businesses will reach 50% by the end of 2017. A 2017 study by Cisco is in a similar vein, finding

that 69% of IT decision makers were in favor of BYOD. What's more, according to Markets and Markets, the BYOD & Enterprise Mobility Market will be worth an eye-watering $73.30 Billion USD by 2021.

IV. 3LEVEL SECURITY

In this paper, we try to provide security for file and folder for providing some idea using 3 levels of password security. That will help to protect the data access from unauthorized person. For that we used following 3 level for security:

There are 3 things that can be used Tablet, Smartphone, Laptop more secure:

1. Use a Strong Password
2. Use a screensaver password, or force the computer to lock itself after a period of inactivity and some time letter if computer is inactive. This provides added protection in case you are away from your device and forget to manually lock it.
3. Protect your web browser with a master password if you have set it up to save passwords and form information.

Following 3levels of security is provided :

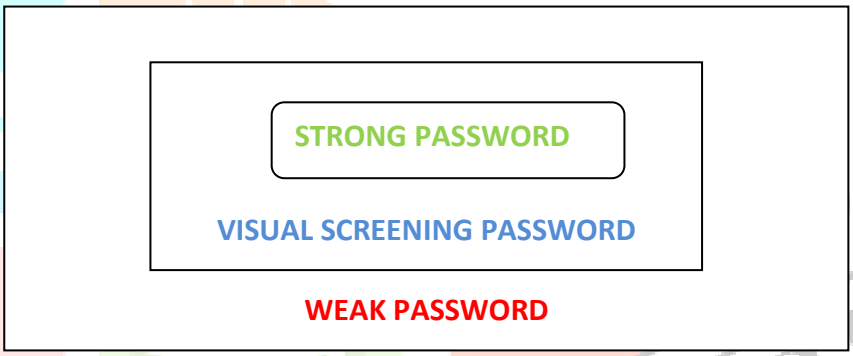


Fig 4.1 Multi-password Technique

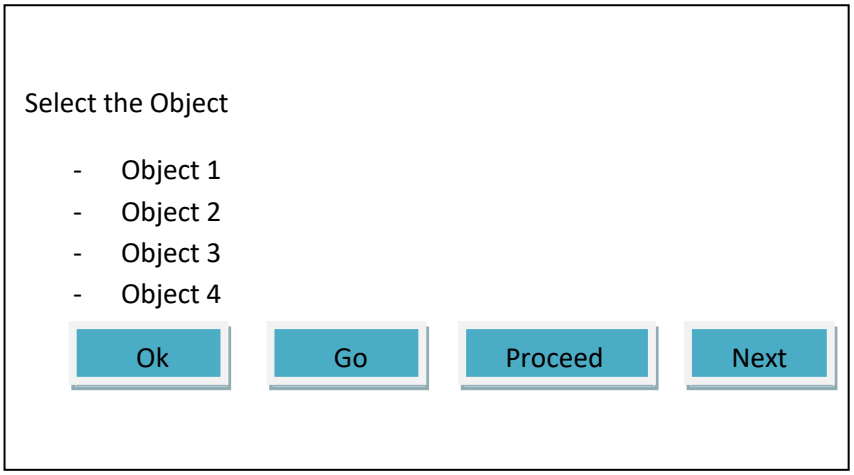
Level 1- Choose a weak password

A password that is easy to detect both by humans and by computer. People often use obvious passwords such as the names of their children or their house number, contact numbers , birth date in order not to forget them. However, the simpler the password, the easier to detect.
Examples of weak passwords: names, nicknames, and variations of names Only numbers.

It helps to unauthorized person to access an data or file, if the device and laptop are stolen. The person first need to crack the home screening password it may be a secured with biometric, fingerprint or password. If person is able to crack that password and access the folder or file they need to crack the password which is given to that folder, that will be a weak password if person can get the password then it goes for the second level security password to accessing the data.

Level 2 - Visual screening password

In visual screening password the screen will be display and the user are randomly select the object if they choose the already set object, as it know only the user what they have to choose from that object. So it helps to user to secure the file and folder.



Level 3 - Choose a strong password

A "strong" password is one that is hard to guess.
Examples of weak passwords: names, nicknames, and variations of names. Any word that can be found in a dictionary – it is common for attackers to try every English word using automated systems this can be done in minutes. Common quotes – "I have a dream" or similar. Common letter to number replacements are not safe either: pa55word will be easily guessed.

To create a "strong" password, make it as random as possible. Use a combination of letters, numbers, and symbols if possible. A common method of creating a reasonably strong password is to pick certain letters out of a phrase.
For example, the password "Ien!tyseb!" was derived from the sentence "I like bacon! It really is the best!" by taking the last letter of every word and including the exclamation marksiii.
As strong passwords are hard to remember, consider using a password database. The strength of your password will depend on the level of security that you need.

The strong password is 16 character password that will be randomly generated by the server by using a various algorithm, that password is only known to the server admin and user. The strong password is changed automatically from the server in every month. It is hard to encrypt the strong password in minimum day's. So that hacker or unauthorized person start again to encrypt the password until they crack the starting character of the password which is again set new so that they start from the beginning.

In step 3 we can use either strong password or 3D password the both are having its own pros and cons

3D PASSWORD:

The devices used most often for IT services are changing from PCs and laptops to android supported mobile devices and tablets. These devices are in the need of hand held for increased portability and usability. These technologies are more convenient than others technologies, but as the devices start to contain maximum amount of important personal information, a better security mechanism is required. Although these solutions were proposed to be viable, major problems could still result when the device itself is stolen or hack by the hacker. By using this Multifactor Authentication in the Single 3D Virtual Environment, We provide enhanced Security for mobile devices and laptops. Initially the user enters 3D Virtual Environment and they are free to use that environment and they will select the objects. 3d password scheme is a new strategy recognition patterns, textual passwords, biometrics and graphical passwords. One of the important concepts of 3d password schema is 3d virtual environment which contains real time object scenarios. Also 3d password is more secure and hard to break.

Fig 4.3 3D password

CONCLUSION

In this paper, the solution for "Bring Your Own Device" problem is identified for data security and give some idea for data security. Implementing a strong password and 3D password technique can help to provide authentication security for the user. However, if another person can get the visual screening password the strong password and 3D password technique prevent an unauthorized user from gaining the access to data. By implementing the 3 level security we can provide the better security for data (files & folders).

There are various another authentication techniques that can be implemented on this, it will require more time to implement. In future work also a brief research was done on 3D password and another authentication technique

REFERENCES

[1] Meisam Eslahi, Maryam Var Naseri, H. Hashim, N.M. Tahir, Ezril Hisham Mat Saad ,

"BYOD: Current State and Security Challenges," https://ieeexplore.ieee.org/abstract/document/7010235/ ,pp 189-192,April7-8 ,2014.

[2] Divya PremChandran, Sailee Sunil Rajeshirke, "Enhancing 3 Level Security using 3D Password" ,pp 1808-1811,2015

[3] Morufu Olalere, Mohd Taufik Abdullah, Ramlan Mahmod, and Azizol Abdullah, "A Review of Bring Your Own Device on Security Issues," http://journals.sagepub.com/doi/pdf/10.1177/2158244015580372, pp 1-10,April-june ,2015.

[4] Farida Jaha, Ali Kartit ,"Pseudo Code of Two-factor Authentication for BYOD", https://ieeexplore.ieee.org/document/8255248/ .2017

[5] Khoula AlHarthy, Wael Shawkat, "Implement Network Security Control Solutions in BYOD Environment", https://ieeexplore.ieee.org/document/6719923/, pp 7-10, 1 Dec ,2013

[6]Prof. P.L. Ramteke, "3D Graphical Password Authentication System", https://www.ijraset.com/fileserve.php?FID=2066 , pp 68-75, 5 May ,2014