IASET: Journal of Computer Science and Engineering (IASET: JCSE)
ISSN(P): Applied; ISSN(E): Applied
Vol. 1, Issue 1, Jan - Jun 2016, 1-4

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

AVOID HACKING DATAS SAFE TO USE SOCIAL WEB ACCOUNTS USING MOBILES

E. MUTHUVEL

Student, Department of Information Technology, SKP Engineering College,

Tiruvannamalai, Tamilnadu, India

ABSTRACT

Each and every person has to use facebook, Gmail, twitter accounts. In that hackers want to access our accounts means we can get the intimation message from mobile to change the username and password from any were from anyplace. Next time hacker wants to access same account means automatically logout that account .Immediately intimate message will be sent to authorized mobile to change the username and password.

KEYWORDS: Avoid Hacking Datas Safe to Use Social Web Accounts Using Mobiles

INTRODUCTION

Most of the organization employees can use certain pc. In that admin can give username and password for certain employees. If someone knows about the username and password means we can get the intimate message from mobile. Now we are implementing this concept to avoid hacking datas or accounts any were from any place through mobiles itself. In that concept we also include that which time the hacker will log in our account in time basis.

Employee Registration

Employee will sign up for any other social web accounts which are used only for our purpose. All the details are stored in any database. This details can be used to check up the registration process from admin sides Itself. Admin can also send security code for particular persons.

LOGIN PROCESS

User can use there signup username and password in the login page. This will check the database. If password is wrong means the sign in page will automatically logout. Because the user can easily identify someone had been access our account. At the time user can only change the username and password from mobile itself. User which time login to change the username and password can also be displayed in login page.

Figure 1: Represents the Login Process

INTIMATION

Intimation process which is using java programming for sending intimation message to mobile from pc whenever sign in login page. This intimation will help us to know the details about timing of login. At the same time the authenticated mail id person will able to log out his/her login page through the mobile .this process of logout will helps to logout the mail login page which is opened by hacker in pc.

CLOUD SERVER

A cloud server is different from a regular server. Because the resources on the cloud server such as computing power and data storage space used more efficiently. And cloud server is dynamic private virtual server and it is partitioned such that it emerges as several servers. Cloud server is a virtual machine that acts in place of the normal physical server. It can be booted independently at the same time user operating system. The advancement in technology has eradicated the distances and enhanced the technological advent towards cloud server.

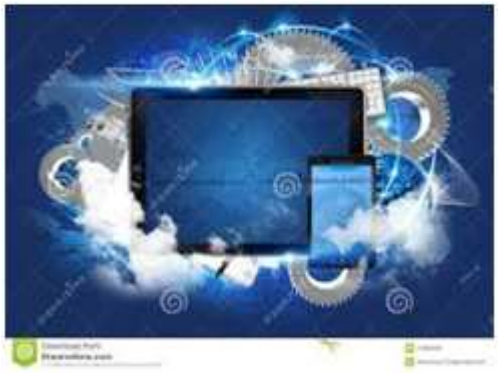

Figure 2: Represents cloud Server to Mobile Clients

HACKER

In the computer security context, a hacker is someone who search and expect weaknesses in a computer system or computer network. Hackers may be encouraged by a huge number of reasons, such as profit, protest, or challenge. The nature, that has evolve around hackers is often get information to as the computer underground and is now a known community. Whenever other uses of the word hacker exist that are not related to computer security, such as referring to someone with an superior understanding of computers and computer networks, they are rarely used in typical context. They are subject to the time-honoured hacker meaning controversy about the true meaning of the term hacker.

SECURITY

Analyse the necessary security for the company, the staff, the resources, the products and the know how. Know about the motivation and plans of e.g. thieves, hackers, irritated employees, organised offense, violent pressure groups, and extremists. Local security negotiator should be asked to provide initial information and preserve a reporting system. Make sure that a security analysis is a original aspect of the overall business stability planning and decisions on all initial expenditures and investments. Determine what is satisfactory and

what is not. It is significant to understand how technical, workforce and managerial means of security act together and help to protected other processes. Make sure that employees, provider and service provider are aware of, and respect the company's security rules and procedures. This information should be a essential part of the "day one" package for new employees and contactors but also for e.g. visitors, possibly in a shortened version. Communications, conversation and information exchanges between stakeholders such as employees, communities, clients, dealer, examine provider and government officials and agencies profile which is maintained in the company database, balanced with safeguards for sensitive information. By the chance this details can be stole and issued to some other company by hacker .so remote monitoring logout method will be helpful to secure the mailing technique in any one organization.

CONCLUSIONS

In every organization each person has some unique username and password. If hacker know our username and password means, there is chance to get the company details and important document or put some unwanted photos or videos from our account. This can be used to get the intimation message to correct user id person mobile, while whenever unauthorized person access another login. At the same time correct user id owner of the person will able to logout and change their password of unique id through mobile. This mobile logout process will automatically log out the pc login page. so the unauthorized person will not able to take the file or document. The unique id will logout and next time hacker will not able to access the account. This method of concept will be prepared by us

REFERENCES

1. M. Armbrust et al., "Above the Clouds: A Berkeley View of Cloud Computing," technical report, Univ. of California, Berkeley
2. V. Kundra, "Federal Cloud Computing Strategy",
3. Cloud Security Alliance, "Security Guidance for Critical Areas of Focus In Cloud Computing.
4. S. Subashini and V. Kavitha, "A survey on security issues in service Delivery models of cloud computing", Journal of Network and Computer Applications

5. I. Burguera, U. Zurutuza and S. Nadjm-Tehrani, "Crowdroid: behaviour based Thefting detection system for android", Proceedings of the 1st workshop on Security and privacy in smart phones and mobile devices

AUTHORS DETEAILS

E. Muthuvel B.Tech, Department of (**Information Technology)** At Skp engineering college (affiliated by Anna University) Contact no: 8608402848