Behavioral Analysis of Students' Login Credentials Management in Mobile Environment

Norliza Katuk [a], Mohamad Subri Halim [b], Hatim Mohd. Tahir [c], Amran Ahmad [d], and Sharmila Mat Yusof [e]
School of Computing
Universiti Utara Malaysia, Malaysia
Email: {[a] k.norliza, [c] hatim, [d] amran, [e] ysharmila}@uum.edu.my, [b] mohamad-subri.halim@hotmail.com

***Abstract*—The number of password-protected Internet-based applications is increasing significantly compared to a decade ago. Consequently, it causes an increase in the number of login credentials that users have to manage, for both Internet ad mobile environments. This paper presents a study that specifically focused on students' login credential management for mobile computing users. A behavioral study was conducted on 250 students from Universiti Utara Malaysia to understand how they managed their login credential while accessing the Internet via their mobile devices. The results suggested that students practiced poor login credential management. The paper recommends approaches that can be taken to improve login credential management for users with mobile devices.**

***Index Terms*— login credentials, password management, mobile environment, Internet usage behaviors**

I. Introduction

The advances in information technology (IT) cause a rapid growth in online and computerized information systems. The major benefit of this trend is that it allows users to perform personal and business transactions easily through the Internet, and at their convenience. As various systems are available online, each of them implements authentication methods to identity the identity of individual users, to keep track of users' data, to protect users' privacy, and to keep users' data confidential. Login credential through combination of user identification (ID) and password is the most common authentication method used in the Internet [1]. In 2007, Florencio and Harley [2] reported that in average, users had 6.2 passwords to access various Internet applications [3].

The number of sites that require users to subscribe to their services is increasing rapidly more than we expected [1]. Bang's study [1] in 2012 revealed that the average number of sites that a user subscribed was 105.7 ranging from the minimum of 29 accounts to the maximum of 199.

Internet applications are now moving towards a new paradigm where users can access them through wireless and mobile devices such as smart phones and tablet PCs. It created a mobile computing environment, where access to the Internet is more flexible than the use of desktop and wired networks. Users who access Internet applications through mobile devices are also exposed to security threats as much as users with desktops and wired networks. Reports on security vulnerabilities such as malware attacks that steal confidential information in mobile devices, and loss or theft of devices have increased the risks. This suggested that mobile environment is also facing security challenges and it is still far from secure [4].

Security protections require organizations and users to take proactive actions to avoid unnecessary loss of data and confidential information. In organizations, a security policy protects users and data, and it guides users on how to behave towards a safe computing environment [5]. In terms of individual users, login credential is a basic step for security protection. However, users often ignore the importance of proper login credential management. Many users practice weak passwords management that could increase security threats in a mobile environment [6].

In this paper, we explained our research that studied students' login credentials management in a mobile environment. We conducted a behavioral study to understand students' Internet usage, their practices on login credentials management, and their security and privacy perceptions. The next section of this paper explains literature related to this study. It is followed by an explanation on the empirical study and its findings. Then, we discuss and conclude the findings in the last section

II. Login Credential Management in Mobile Environment

Mobile computing is increasingly popular among young generation of Internet users. Further, mobile phone users who connected to the Internet are much higher than desktop users with the most popular application is the social networks [7]. Apart from social networks, users also accessed emails and performed online banking and commerce transactions through mobile devices. As many applications are available through mobile devices, data exchange between users can be a source of security attacks and threats.

Internet and mobile application providers protect their data and systems from security attacks by implementing user authentication. Authorized users can access the specified resources or perform transactions by providing login credentials to the systems. The combination of user

Manuscript received June 24, 2013; revised August 15, 2013.

doi: 10.12720/jiii.1.3.132-138

ID and password is the most common user authentication method for mobile and Internet applications.

A. Security of Login Credentials

Authentication of users' identity in mobile and internet applications plays two important roles. First, it acts as a security method to authenticate access from authorized users, and second, it is a way to recognize users' preferences and characteristics that act as a method to provide them with personalize contents. Both reasons have made applications providers implement user authentication. Consequently, the number of Internet and mobile applications requiring registration has dramatically increased.

This imposes a new challenge to users, as they need to keep a lot of login credentials to get access to the applications. It is critical when users are unable to manage their login credential effectively that demanded for a new alternative approach of its management. Having multiple login credentials is not only a bothersome aspect of the Internet and mobile environment; it is also one of the most serious security issues that has been continuously debated. When a user has a number of login credentials, how he or she manages them is always been an issue. The user tends to write them on paper, or keep them stored in the mobile devices. Another potential behavior is reusing or repeating the same login credential on many different applications. Any of this behavior is actually exposed users to various security attacks.

It is important to realize that a strong security protection does not guarantee that a particular system is secure. This is definitely true when the users' practices and behaviors do not bother with it. Mistakes due to users' malpractices and behaviors are the easiest point of attack in computer systems. Hence, it can be said that, security is only working when both technical and users' behavioral perspectives are there at the same time [1, 8].

Good login credential management practices are important to ensure that systems and application are secure. The practices include regular change of the password, use non-dictionary word for the password and combining password with special characters.

B. Related Studies

Many past studies in the area of computer security were more focusing on users' behaviors in the Internet environment. Users' behavioral studies within a mobile environment are still new, and not much attention has been given to this particular domain. The following paragraphs discuss studies that particularly related on Internet users' login credential management.

Bang et al. [1] studied Korean Internet users' behaviors specifically on their login credential management. Their study revealed that user's behaviors make their login credentials vulnerable and susceptible to attacks. This is particularly true when users replicate the same login credential for many unsecure online systems. This practice also jeopardizes other secure online systems, as the replicated login credentials can be used by cyber criminals as a tool to penetrate them. The results of Bang's study proposed two important points to organization and government agencies, (i) the needs for formulation of a security policy that prevents users from replicating their login credentials, and (ii) the needs for new authentication methods other than remembering login credentials.

Tam et al. [9] conducted a study to understand whether users are aware of the good password management practices and how do they behave towards it. They conducted an experimental study on 140 Internet users. The results of their study revealed that users were aware of the characteristics of good and weak passwords. However, they tend to practice bad password management because they did not see and anticipated the immediate consequences of those practices. They rather see that other people would get the consequences of bad login credential management than themselves. The result also suggested that users tend to go for convenience-security trade-off.

Kumar [10] conducted a survey in India investigating the usability of alphanumeric passwords. In his study, he found that alphanumeric passwords are difficult to remember causing users to write them down on papers. The study suggested that usability can be a security tradeoff. Although alphanumeric passwords can be considered as robust against attack, however, many users are unable to remember them. Consequently, they wrote the password on papers.

The three studies discussed above show users practiced weak login credential management by replicating the same passwords in different applications, use weak password, and write down the passwords on papers. These are common users' behaviors when they access the Internet through a wired network. In the context of mobile computing, we wonder how users behave. Hence, the following sections explain our study to understand how users manage their login credential and how they behave in a mobile computing environment.

III. Methodology

A. Method and Procedure

A self-report study was conducted as the main research method. The participants were asked to fill-in a self report questionnaire to assess their login credential practices. They completed the given task in a large seminar hall within a researcher's supervision. They were asked to return the questionnaire to the researcher before they left.

B. Respondents

A number of 250 students of Universiti Utara Malaysia from various programs (e.g., Business, Accounting, Economic, Linguistic, Finance, Social works, etc.) participated in this study during October to November 2012. The researchers asked permission from selected instructors who taught IT Fundamental course to recruit students from their classes. Students received no compensation for their participation. Past research had proven that university students are the heavy users of mobile devices [11], hence making them appropriate to be the targeted group for this study.

C. Materials

A close-ended questionnaire was designed according to common questions that had been asked in other past studies pertaining login credential practices. It was divided into 4 parts as follow:

i) Part I- Demographic information (6 questions)
ii) Part II- Mobile devices and Internet behavior (4 questions)
iii) Part III- Login credential management (5 questions)
iv) Part IV- Perception on security and privacy (7 questions)

IV. Results and Findings

A. Demographic Information

Fig. 1 shows the demographic information of the respondents. In total, 78.4% female students participated in the study. In terms of the respondents' age, 99% of them were below 25 years with the mean age of 21.25. The majority of them were undergraduate students from different number of semesters and courses.

B. Mobile Device and Internet Usage Behaviors

In studying behaviors of the students, we first asked them on their mobile devices ownership. The pie charts in Fig. 2 show that 89% of the students (approximately 223 students) own mobile devices with Internet connectivity including smart phones, tablets, netbooks, and laptops. Out of this number, 56% had only one mobile device, 33% had two mobile devices, and 5% had 3 or more devices. About 6% of them did not answer the question.

We also investigated how long the respondents spent their time accessing the Internet. The bar chart in Fig. 3 shows the information. 41.6% of the respondents spent more than 4 hours a day connecting to the Internet, 21.2% and 20.4% used the Internet between 2 – 3 hours, and 3 – 4 hours a day respectively. Less than 6% had accessed the Internet less than an hour a day.

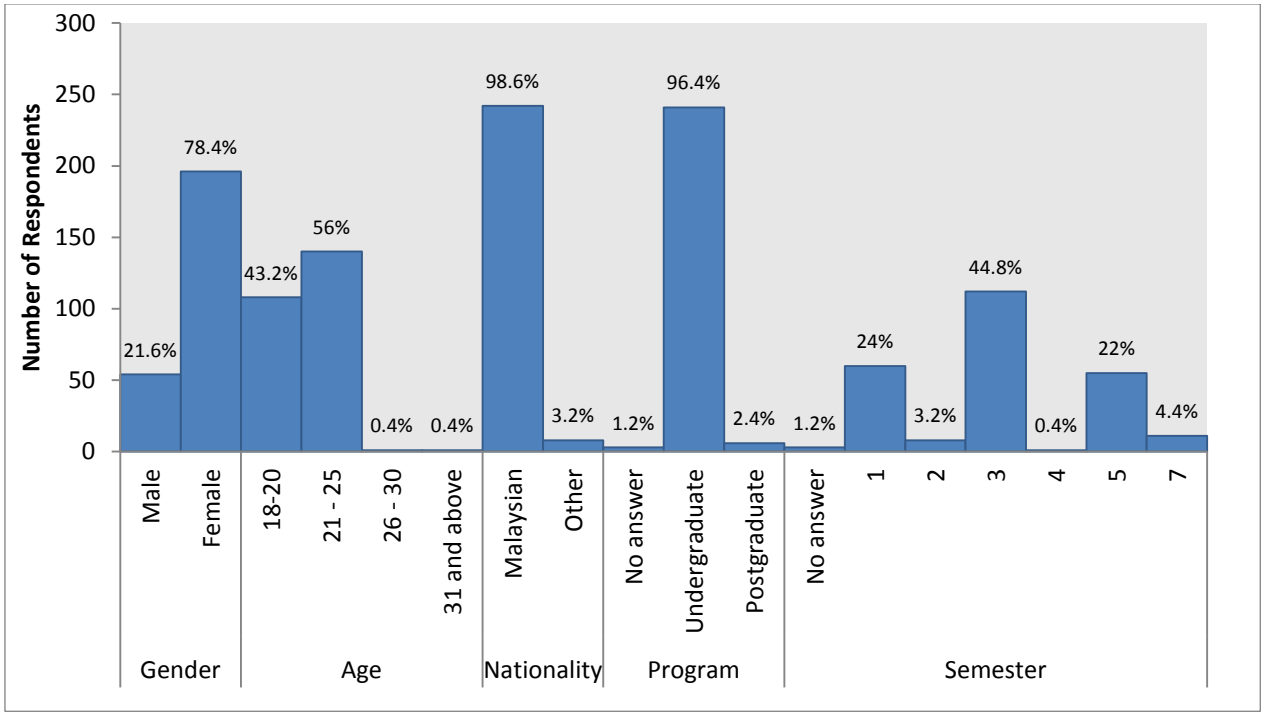
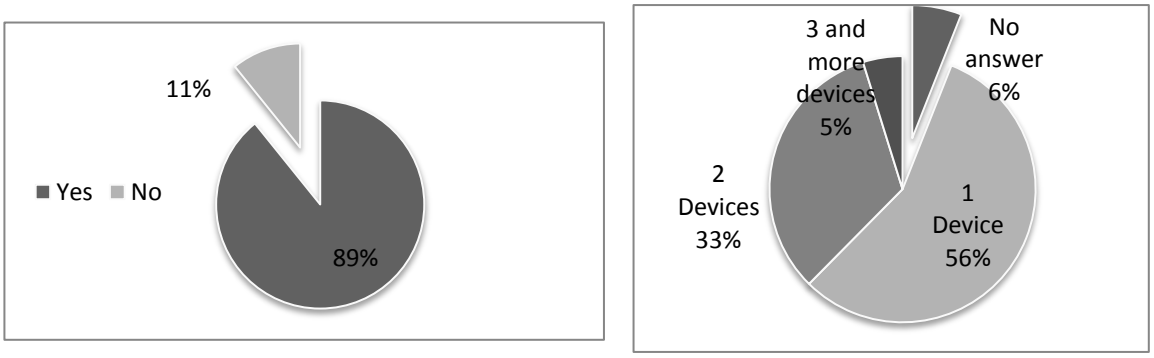


Figure 1. Demographic information



a) Students own mobile devices with Internet connectivity b) Number of mobile devices owned by the students

Figure 2. Mobile devices ownership

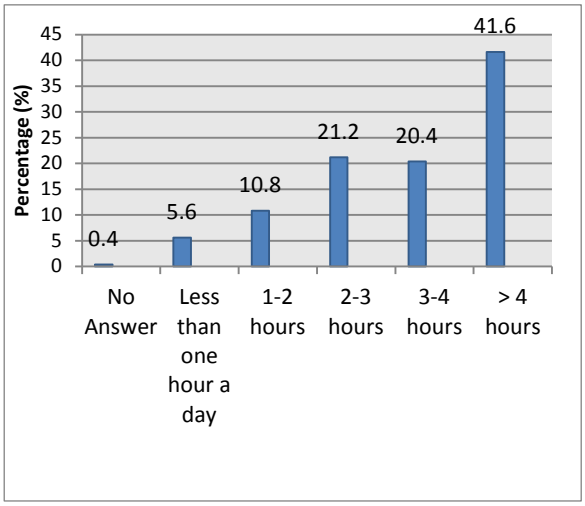


Figure 3. The duration of access to Internet daily

We also investigated the type of Internet resources that the respondents accessed. The respondents were asked to choose the top three Internet resources that they frequently access every day. Fig. 4 below shows that the majority of the students used the Internet for social networking with 216 counts. The result also revealed that web browsing, music, news and file sharing also popular within the sample.

C. Login Credential Management

In order to understand the students' behaviors on login credential management, they were asked on how many login credential they have at the time this study was conducted. All respondents had at least an email account and a web login, and the maximum of eight accounts respectively with the password length was within 6 – 15 characters. Fig. 5 shows how the students managed their login credentials. More than half of the respondents (61%) used the same usernames and passwords for accessing multiple applications. Only a small number of students (37%) used different passwords to access different applications. On the other hand, 64.8% of the respondents never changed their passwords. Nevertheless, some respondents changed their passwords once a year (20%), 10.4% of them changed their passwords every six months, and 4% every month. Only 0.8% changed their passwords every week. Although some respondents concerned about the password security, the study found that 25.2% of the respondents shared their passwords and mobile devices with other people (e.g., family, spouse, etc.).

This study also revealed that the students created a weak password based on surrounding objects or personal information which can be guessed by people who know enough about them. These weak passwords include date of birth, nickname, parents' names, or celebrities name or any favorite pets.

D. Perception on Security and Privacy

The respondents were also asked on their perception about security and privacy. Fig. 6 shows their responses. More than 70% of the respondents were concerned about privacy on the Internet. However, 9.2% of the respondents indicated that they were "less concerned" about their privacy while using the Internet.

This study also examined students experience whether they had been asked to provide personal information by the visited websites. Majority of the respondents (76.8%) had experienced it. Interestingly, 39.2% of the respondents chose to give fake information to the websites that requested for their personal information, and 14% chose to provide their real personal information. More than a half of the respondents (54%) were reluctant to provide their personal information.

In terms of supplying personal information for advertisement, the findings of this study suggested that 44.4% of the respondents were not willing to provide personal information for online advertising purposes. Further, half of the samples read the terms and conditions of web policies before they provided the personal data to particular websites, while the other half never read them.

60.8% of the respondents had never been contacted by strangers as a result of providing data for advertisement. While 24% experienced it, 13.6% did not remember such incidents. More than 70% of the respondents believed that many people can view their personal data if they place them on the Internet. However, in response to the question about security measure for personal data protection, only 54.4% performed some security and privacy protection, while 17.2 % did not take any security measure. A portion of 26.8% did not know how to do it.

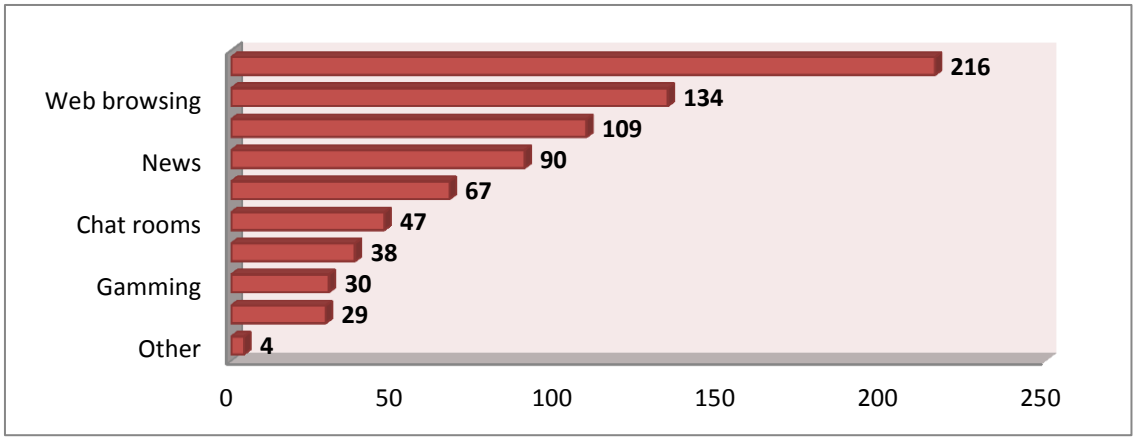
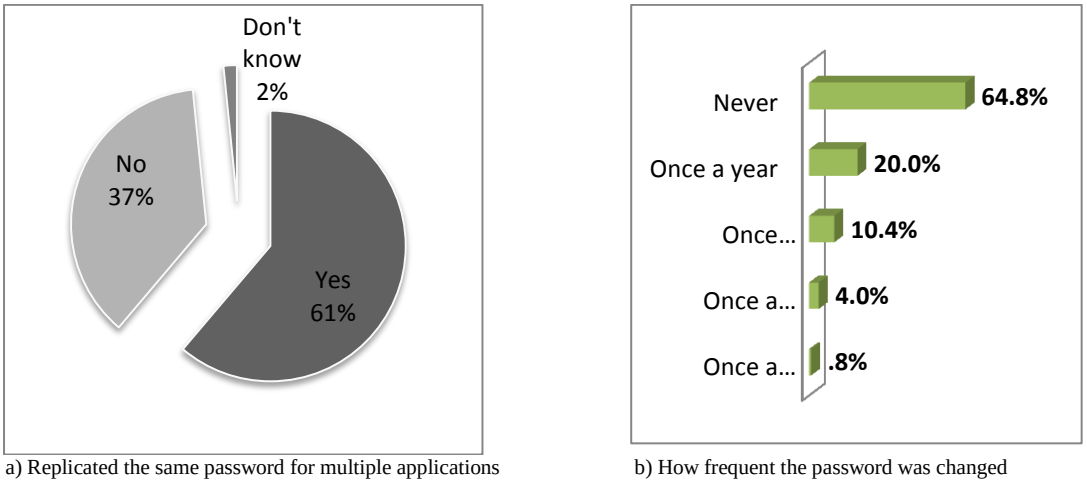


Figure 4. Types of Internet recourses that the students accessed



a) Replicated the same password for multiple applications

b) How frequent the password was changed

Figure 5. Login credential management

V. Discussion and Implications

Mobile devices began a worldwide revolution when they provide users with the first time experiences connecting online away from computer and wired Internet connections. The development of smart phones and other gadgets took the power of mobile technology a step further and shifted students expectations for accessing digital content. With the increase of mobile technology such as smart phones and tablet PCs, it may also give rise to privacy and security threats. Nowadays, the traditional authentication method such as username and password are no longer sufficient to cope with the latest security threats. Therefore, strong authentication scheme becomes more relevant with the current Internet technology.

A. Internet Usage Behavior

This study revealed that the majority of the students owned at least one mobile device with Internet connectivity. It is also suggested that the students were heavy Internet users, where half of them spent more than four hours a day accessing the Internet from their mobile devices. The majority of the students accessed social network sites especially Facebook when they online. The Internet usage confirms that students show addictive and habitual behavior [11]. Shambare et al. [11] suggested that these two behaviors are associated with frequent used of mobile devices among students. Accessing the Internet has become the major focus of a person's life more than other activities and it is performed regularly and repetitively.

B. Login Credential Management

In terms of login credential management, a few interesting results have been found. This study suggested that two-thirds of the students never changed their password, and similarly, they replicated one single password in many Internet applications. This critically shows that the students did not practice proper login credential management. This finding confirms the results of a past study by Bang *et al*. [1] that found a similar behavior among students in terms o their login credential management. They explained that users tend to replicate their passwords due to limited memory capability that a human has. It is a common cognitive theory on human memory [12]. When more sites require users to create passwords, their mind requires more mental process of searching and retrieving the passwords. Consequently, human mind is unable to remember each and every one, hence making users to simply reuse the existing passwords.

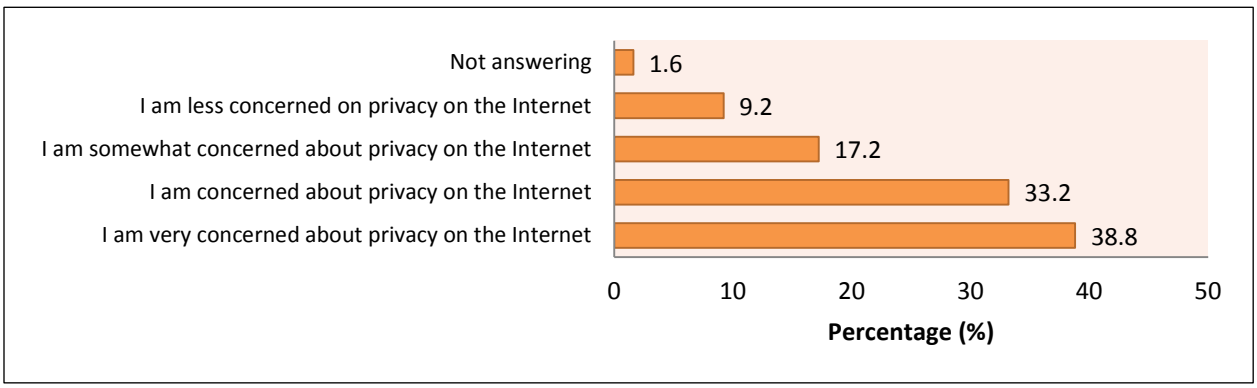


Figure 6. The students' perceptions on Security and privacy

From this study, it is also discovered that a quarter of the respondents shared their passwords with other people including family members and friends. Although it is relatively a small percentage, this result shows that they were not fully aware of the threats that may rise from their actions. Password security is compromised if a cybercriminals learn a single word from it. They will be able to perform various security attacks such as impersonate the user, and access the resources to which this user entitled.

Another important finding of this study shows that the students created their password based on surrounding objects that can be easily broken through brute-force attacks.

The above evidence suggests that the students' practices did not comply with common security guidelines such as a password should be at least eight characters long, user should use different password for each login account, and change them regularly. Although the students were aware that they have to protect the privacy of their personal data, their behaviors and practices on the login credential management did not align with their perceptions. We are interested to study in the future, why do students' behave far away from what they thought in terms of the security aspects. We hypothesize that students' behaviors are influenced by their attitude and perceived norms.

C. Approach to Increase Login Credential Security

As mobile computing is increasingly popular among Internet users especially students, proactive actions should be taken to increase the security of its resources. Based on our findings, we suggest the following managerial and technological approaches to increase security and to promote good practices of login credential management within a mobile environment:

i) *Training.* Students' practices and behaviors on their login credential management are insufficient and weak. Hence, proper training and awareness programs must be implemented to improve this condition.
ii) *IT Policy.* The existing security policy should be modified in such a way that it promotes good security practices, such as regular password change and enforcement of long and secure passwords.
iii) *Single-sign-on (SSO) [13]*. SSO could be an alternative to avoid students from replicating their passwords in different applications. SSO technology and protocol such as OpenID and SAML [14-16] are available, and they can provide better login credential management to users.
iv) *Biometric authentication.* The use of biometric authentication [17] such as finger print could be an alternative to login credential for a mobile computing environment as it could increase the efficiency of identity management.

The above approaches play two-fold roles. Training and IT Policy can be seen as managerial approaches that can educate students to change weak login credential management practices. On the other hand, SSO and biometric authentication are the technological approaches that can facilitate login credential management and as well as strengthen the security of mobile computing applications.

ACKNOWLEDGMENT

This work was supported in part by a grant from Universiti Utara Malaysia (LEADS –S/O Code: 12397).

REFERENCES

[1] Y. Bang, D. J. Lee, Y. S. Bae, and J. H. Ahn, "Improving information security management: An analysis of ID–password usage and a new login vulnerability measure," *International Journal of Information Management*, vol. 32, pp. 409-418, 2012.
[2] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings 16th international conference on World Wide Web*, 2007, pp. 657-666.
[3] M. Jakobsson and M. Dhiman, *The Benefits of Understanding Passwords*, Springer, 2013.
[4] A. Jain and D. Shanbhag, "Addressing security and privacy risks in mobile applications," *IT Professional*, vol. 14, no. 5, 2012.
[5] L. Karadsheh, "Applying security policies and service level agreement to IaaS service model to enhance security and transition," *Computers & Security*, vol. 31, pp. 315-326, 2012.
[6] T. Matthews, "Passwords are not enough," *Computer Fraud & Security*, vol. 2012, pp. 18-20, 2012.
[7] C. Mascolo, "The power of mobile computing in a social era," *Internet Computing, IEEE*, vol. 14, pp. 76-79, 2010.
[8] B. Y. Ng, A. Kankanhalli, and Y. Xu, "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems*, vol. 46, pp. 815-825, 2009.
[9] L. Tam, M. Glassman, and M. Vandenwauver, "The psychology of password management: a tradeoff between security and convenience," *Behaviour & Information Technology*, vol. 29, pp. 233-244, 2010.
[10] N. Kumar, "Password in Practice: an Usability Survey," *Journal of Global Research in Computer Science*, vol. 2, pp. 107-112, 2011.
[11] R. Shambare, R. Rugimbana, and T. Zhowa, "Are mobile phones the 21st century addiction?" *African Journal of Business Management*, vol. 6, pp. 573-577, 2012.
[12] R. E. Mayer, "Cognitive theory of multimedia learning," *The Cambridge Handbook of Multimedia Learning*, pp. 31-48, 2005.
[13] S. Suriadi, E. Foo, and A. Jøsang, "A user-centric federated single sign-on system," *Journal of Network and Computer Applications*, vol. 32, pp. 388-401, 2009.
[14] A. Armando, R. Carbone, L. Compagna, J. Cu ellar, G. Pellegrino, and A. Sorniotti, "An authentication flaw in browser-based Single Sign-On protocols: Impact and remediations," *Computers & Security*.
[15] OpenID. (2013). The Benefits of OpenID. [Online]. Available: http://openid.net/get-an-openid/individuals/.
[16] V. Radha and D. H. Reddy, "A Survey on Single Sign-On Techniques," *Procedia Technology*, vol. 4, pp. 134-139, 2012.
[17] S. Furnell, N. Clarke, and S. Karatzouni, "Beyond the pin: Enhancing user authentication for mobile devices," *Computer Fraud & Security*, vol. 2008, pp. 12-17, 2008.

Norliza Katuk was born in Johor, Malaysia on 1st October 1978. She obtained her Bachelor's degree in information technology from University Utara Malaysia in 2000 and her Master's degree in computer science from Universiti Teknologi Malaysia in 2002. She obtained her Doctoral degree in information technology from Massey University, New Zealand in 2012.

She started her career as a Tutor at Universiti Utara Malaysia in 2000 and is currently a Senior Lecture there. Her research interests cover multidisciplinary areas including information security and privacy, web-technology, disaster management and human-computer interaction. Dr. Norliza is an editorial board member of Journal of ICT, Universiti Utara Malaysia.

Mohamad Subri Halim received his Bachelor's and Master's degrees in information technology from Universiti Utara Malaysia in 1999 and 2012 respectively. During the last fourteen years, he worked in multinational companies including Intel Corporation. He is currently pursuing his PhD in computer network at Universiti Utara Malaysia. His research interests include future network, named data network, and enterprise network.

Hatim Mohamad Tahir received his Bachelor's and Master's degrees in computer science from Northrop University, (USA) and Indiana State University, (USA) respectively.

He is currently an Associate Professor at the School of Computing, University Utara Malaysia. He has written and published books on data communications and security namely, Data Communication and Server Security. He also won several awards in Malaysian Technology Exhibitions (MTE), International Exhibition and Innovation Exhibitions (ITEX), Institution of Higher Learning R & D Exhibition (PECIPTA) and Seoul International Inventions Fair (SIIF).

His domain area of research is focusing on intrusion detection prevention system (IDPS), mobile ad-hoc network security and information security. He was formerly a member of the Panel of Expert (PoE) for Malaysian Cyber Security (formerly National ICT Security Emergency Response Center - NISER). Assoc. Prof. Hatim is also a member of various ICT and Security related organizations. Currently, he is also a member of the National R&D Roadmap for Self Reliance in Cyber Security Technology and Malaysian Research Document Classification System (MRDCS) under the Ministry of Science, Technology and Innovation (MOSTI).

Amran Ahmad was born in Kedah, Malaysia on 25th August 1971. He received his Bachelor's and Master's degrees in information technology from Universiti Utara Malaysia in 1995 and 2003 respectively. He is a lecturer and currently doing his PhD study there.

He did a research in business intelligent in 2002, wired network vulnerability assessment in 2004, open source server services in 2005, wireless network vulnerability assessment in 2010 and setting up grid site for knowledge grid Malaysia in 2012. He also published many articles in journals and conference proceedings in the area of computer networks.

Mr. Amran is a member of Internet Society Malaysia. He was also awarded Bronze Medal at Research & Development Expo 2005, Kuala Lumpur, on his group project on Server-Based Open Source System Implementation for ICOSYS.

Sharmila Mat Yusof was born in Kedah, Malaysia on 25th March 1973. She obtained her Bachelor of Science degree in Computer Science (1996) from the University of Missouri Kansas City, United States. She obtained her Master's degree in Information Technology (2006) from the Universiti Utara Malaysia, Malaysia and is currently a candidate for a Doctor of Philosophy (Ph.D.) in Database Systems at Universiti Putra Malaysia, Malaysia.

As a lecturer at Universiti Utara Malaysia, she specializes in Database Systems, System Analysis and Design and Management Information Systems. At present she is currently a lecturer at the School of Computing, College of Art and Sciences, University Utara Malaysia. Before joining the educational field, Mrs. Sharmila has an industrial experience as an analyst programmer and system analyst in the fields of telecommunication and transportation. Her skills include programming in Visual Basic, Java, database scripting in MySQL and proficiency in MS office tools such as MS Access and Project. Her research interests are database system, data warehouse modeling, OLAP tools and ontology.