Security and Privacy Risks Awareness for Bring Your Own Device (BYOD) Paradigm

Manmeet Mahinderjit Singh, Chen Wai Chan and Zakiah Zulkefli
School of Computer Sciences, Universiti Sains Malaysia, 11800 Penang, Malaysia

***Abstract*—The growing trend of BYOD in the higher education institutions creates a new form of student learning pedagogy in which students are able to use the mobile devices for their academic purposes in anywhere and anytime. Security threat in the paradigm of BYOD creates a great opportunity for hackers or attackers to find new attacks or vulnerabilities that could possibly exploit the students' mobile devices and gains valuable data from them. A survey was conducted in learning the current awareness of security and privacy importance in BYOD for higher education in Malaysia. Based on the analysis of this survey, it demonstrates that the trend of BYOD in Malaysia has begun. Thoroughly, the survey results have been proven that the current basic fundamental security and privacy awareness and knowledge on mobile devices or applications is important in order to protect their mobile devices or data.**

Keywords—Mobile Computing; BYOD Higher Education; Security; Privacy; Malicious Software; Risk

I. INTRODUCTION

A tremendous growth in lightweight, portable computing devices and wireless communications has made mobile computing becomes a next-generation computer technology that would transform the way of people interact with each other not just in their daily life, even in their student life. Smartphones, tablets, PDAs, USB memory drives are the perfect examples of mobile computing devices. These devices are equipped with services such as file transfer, internet browsing, mailing services and web-based applications, where these services allow the users to access data or information and collaborate with each other on the move [1]. Thus, there is an increasing use of mobile computing devices among students for their higher education purposes as these devices provide an opportunity for better productivity, performance, convenience and also a promise of mobility [1]. This phenomena leads to a trend which is known as Bring Your Own Device (BYOD) Higher Education, where students are allowed to bring their own devices into their study place and they can perform their educational activities through their own devices.

The increasing use of mobile devices or apps among the students and the growing popularity of the BYOD Higher Education have led to a serious security and privacy attacks towards the campus data and network as well as student's personal information stored on their devices such as student's records, grades, financial and research information and etc. For example, spear phishing [2], Advanced Persistent Threat (APT) attack [3, 4] and malware [4] are the potential attack vectors for BYOD models. Other than that, most of the educational institutions have allowed some form of BYOD trend onto their campus via Network Access Control (NAC) without implementing any organized BYOD policies. This approach poses risk towards the institution's networks as well as student devices such as unauthorized access, attacks of malware and viruses, loss of data and etc. [5].

Thus, the main aim of this study is to observe the awareness of BYOD paradigm and the security and privacy threats that occur within this environment. The objectives of the survey are 1) to investigate the growing trend of BYOD Higher Education and 2) to examine the student's security and privacy knowledge and awareness on mobile devices or applications. The significance of the survey is to understand the perception of the current generation Y on the concept of BYOD and its security challenges that comes with it.

The remainder of the paper is structured as the following. Section 2 covers the background study of BYOD and its security and privacy issue in higher education. Section 3 focusing on BYOD survey conducted to increase the user awareness. Section 4 and 5 are respectively provided a discussion on the survey and the conclusion thoroughly.

II. BACKGROUND AND RELATED WORKS

This chapter comprised of three parts included BYOD in higher education, m-learning adoption and security and privacy risks on BYOD.

A. BYOD in Higher Education

Bring Your Own Device (BYOD) Higher Education refers to the practice of higher education students using their own mobile computing devices in their lecture hall or classrooms. Traditionally, BYOD devices include laptops, PDAs, but recently the growing usage of smartphones and tablets have become a part of BYOD devices which offers a high degree of mobility and flexibility. Yu [6] observed that there are three major ways where smartphones were being used in higher education, such as using inbuilt web browsers to access educational materials through online, and using mobile applications to access and interact with a course or lecture content. There also have other uses of smartphones such as recording lectures and seminars, participating in-class polls, logging academic data, taking notes, scanning documents and etc. Tablets such as Apple iPad, Amazon's Kindle, and Samsung Galaxy Tab offer students and lecturers a portable tool by expanding the connectivity and mobility of smartphones through a larger screen and processing power. Johnson, et al. [7] have defined the uses of tablets in education with this statement: "… have gained traction in education

This work is supported by the Fundamental Research Grant Scheme (FRGS) of Universiti Sains Malaysia.

because users can seamlessly load sets of apps and content of their choosing, making the tablet itself a portable personalized learning environment".

B. M-Learning Adoption

According to Akour [8], there are various important factors that influence the acceptance of mobile learning among university students, such as student readiness, ease of access, quality of services, extrinsic influences and institutional commitment. In Lippincott [9], it's believed that the increased capabilities of mobile devices could lead to a new form of engagement with student learning pedagogy. The author also states her belief that student use of mobile devices in higher education correlates to their major area of study as well.

Nowadays, mobile services are provided widely in many universities, for example Massachusetts Institute of Technology (MIT), Stanford University, Harvard University and etc. Besides, the use of mobile learning (m-learning) services in higher education are also becoming one of the active topics in research [10]. In Alzaza and Yaakub [11], the authors explain that the concept of m-learning is considered as the next form of e-learning using mobile technologies so that teachers and learners are able to conduct their learning process in anywhere and anytime. In addition, the authors also conducted a study on the students' awareness and requirements of mobile learning services among Malaysian students in the higher education environment. The results indicate that the students have adequate knowledge and awareness to use the mobile technologies as their choice of the learning environment. M-learning also provides various advantages including freedom to study, low cost, timely application [12], authentic and reliable learning situations, ease of use, support in learning situations [13] , fast production of digital learning materials and flexibility of learning [14].

M-learning could provide lecturers to encourage students to use their devices and some collaborative tools that they support in order to work together on assignments in both physical and virtual learning environments [15]. Other than that, some of the mobile applications could increase the interaction between students and lecturers through an in-class tasks, where it allows students to learn in their preferred places and foster a student-centered learning approach [16].

C. Security and Privacy Risks on BYOD

In this section, security and privacy list will be discussed thoroughly.

1) Installation of malicious software on BYOD

According to Bandara, Ioras, and Maher [17], university and college students are the biggest user of social media or social networking apps such as Facebook, Twitter and YouTube. However, this can lead malwares and viruses such as Wildfire, hosting and spreading throughout the student's personal devices. Bradley, Loucks, Macaulay, Medcalf, and Buckalew [18] explained that an accidental malware downloads not only infects the device itself, it also can easily spread to an entire organization's network within a few seconds. A common mobile malware attack such as Dream Droid [19] and DroidKungfu [20] are luring users to click on malicious web links from their smartphones' web client and install malicious payloads. Moreover, BYOD can easily targeted by hackers to break into someone's devices by sending malicious software through email or application download [21] , for example, hackers always lookout for an opportunity to fool the students through using email or web accounts to spoof the official school mailings as well as bank accounts.

Therefore, students may be encountered the risk of being the victim of a phishing scam that will result in malware or ransomware downloads [22]. As a result, once the student has download and execute malware, the possibility of leakage of student's personal information will increase and the ability of the attacker to steal sensitive information by installing backdoor on the campus network will become possible.

2) Use of untrusted mobile OS and applications

With a "hacker" culture has arisen among young adults, especially when the majority of them are considered as "tech-savvy" nowadays, some of the students used to play with their mobile devices and they able to disable the native OS security feature through the techniques which commonly known as "jailbreaking" or "rooting". By jailbreaking or rooting their mobile devices, they allow installing or upgrading their mobile OS and applications for free that are restricted by default [23]. However, jailbreaking or rooting enables unauthorized programs to be installed on mobile devices, which could probably introduce malware into their devices. This might cause students' devices to be compromised as well as the campus network if student connects his or her devices to the campus network. Besides, some students intend to bypass the institution's proxy servers and access to blocked sites through the mobile VPN and some of them may install some applications such as games, entertainment apps, and P2P video streaming apps which has been restricted by the university. In this instance, it potentially opens up a security threat to the campus network as well as the student's personal data [24].

3) Use of untrusted networks

According to Paullet and Pinchot [25], the mobile devices can be used on both secure and unsecure environments. When users connect their devices to an unsecure network such as public Wi-Fi, the devices will open for a variety of security and privacy attacks such as Wi-Fi hijacking, Bluejacking and etc. For example, Wi-Fi hijacking occurs when a hacker is able to intercept the communications between smartphones and unsecured Wi-Fi hotspots, which allows hackers to gain access to someone's usernames, passwords if a user logs in to certain mobile apps or web site. Therefore, students should be alarmed of the potential risk as many mobile devices have settings to allow the device to automatically connect to available rogue wireless access point that might controlled by hackers [26]. Other than that, forward emails to public Web mail services over the cellular network via BYOD, synchronize academic documents using public cloud-based storage services like Dropbox, iCloud and Google Docs, and interact smartphones through voice in the public place may lead to sensitive data leakage [27].

4) *Lack of physical security controls*

Since the BYOD adoption in the higher education allows students to bring their personally-owned devices into their study place, there is a risk of loss of student personal data will be occurred due to BYOD devices are easy to lose or steal within the campus or in the public. Furthermore, it also places an additional risk to the educational institutions as BYOD devices could contain student's credentials to access sensitive institution's resources or data and also could lead to these data being compromised or malicious activities executed via mobile devices that could gather or corrupt data as well [28]. There's also a possibility that an attacker could configure another device to be a duplicate of a legitimate device which appeared to be authentic to the campus network and steal all the information once the cloned device able to access into the network [23].

5) *Privacy risks on BYOD*

In term of BYOD, the privacy aspect always refers to the concerns that the private data such as personal emails, photos, videos, bank statements, social security numbers, chat histories, usernames, passwords and other credentials are exposed to outsiders. While in the context of BYOD Higher Education, sensitive data such as student's personal details and communications, confidential information about students, assessment data, and confidential institutional data and even the personal credentials for certain educational mobile apps or social networking apps could be exposed to various privacy issues. In Ismail et al. [29], the author states that students are concerned about their privacy and security when they are using m-learning or educational applications, they are worried that their confidential information such as assessment results might be revealed to others.

Besides, the issues of mobile bullying or cyber bullying exist within the educational institutions as the mobile devices can be used for bullying other students and teachers. Some mobile bullying examples like photographing or videotaping other students or teachers and publicly posting, sending or forwarding their photos and videos on the social networking site, websites, emails or message boards in order to harass or humiliate them. Some people even get access and copy or delete someone's information like electronically submitted or stored assignments and homework, or important emails. In addition, some bullies also try to impersonate or pretend to be someone where his or her account has been hacked in order to send abusive calls, texts or images through a mobile phone. This would properly pose a privacy threat to students and teachers personal mobile data.

Other than that, the device location tracking issues also one of the serious privacy issues for the context of BYOD. Although location tracking via a mobile device's geolocation service or GPS are useful for locating lost devices, but illegitimate tracking can cause a serious privacy concern for mobile users. Mobile device tracking or location snooping may expose a threat for students as their location has been recorded and potential criminals will spy on the targeted student's daily activities and perform their crimes. Nowadays, many legitimate or third-party mobile apps provide not just the capability of device tracking, it also allows the tracking of mobile usage behavior tracking via the installed application. This means that the installed apps allow the tracking of selected events occurred on mobile devices and recording every action taken by mobile users [23]. This probably poses another privacy threat to the student if they installed a variety of third party apps.

III. SURVEY ON SECURITY AND PRIVACY AWARENESS FOR BYOD HIGHER EDUCATION

The aims of designing this survey are:

- To investigate the growing trend of BYOD Higher Education.
- To examine the student's security and privacy knowledge and awareness on mobile devices or applications.

Fig. 1 provides an overview of the survey samples, methods and variables used in this research work:

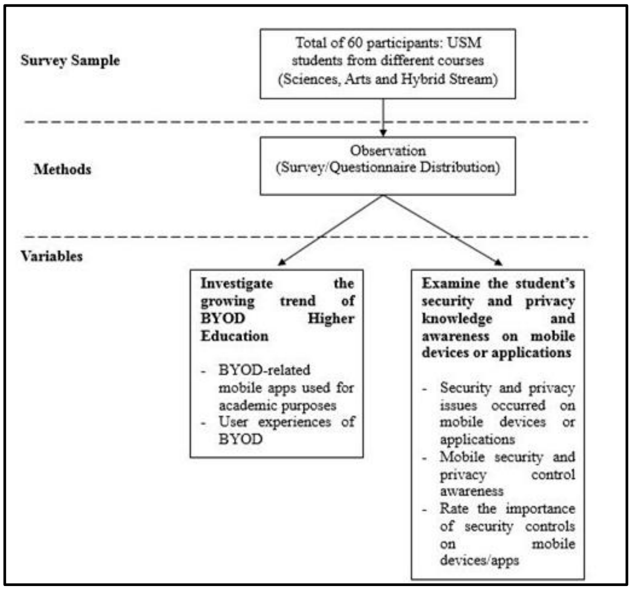
Survey Sample
Total of 60 participants: USM students from different courses (Sciences, Arts and Hybrid Stream)
Methods
Observation (Survey/Questionnaire Distribution)
Variables
Investigate the growing trend of BYOD Higher Education
- BYOD-related mobile apps used for academic purposes
- User experiences of BYOD
Examine the student's security and privacy knowledge and awareness on mobile devices or applications
- Security and privacy issues occurred on mobile devices or applications
- Mobile security and privacy control awareness
- Rate the importance of security controls on mobile devices/apps

Fig. 1. Survey sample, variable and methods

In this research, a data collection method has adopted: Observation. Observation is the method that the compilation of data collected through questionnaires or survey. For example, an online survey will be generated, conducted, distributed and get responses through online. As a result, a total of 60 university students of different courses from the University Sains Malaysia (USM) have taken part in this survey regarding the security and privacy of BYOD Higher Education, where 39 of them are males and 21 of them are females.

IV. SURVEY RESULTS AND FINDINGS

In this section, the survey findings will be displayed.

A. *Investigate the Growing Trend of BYOD Higher Education*

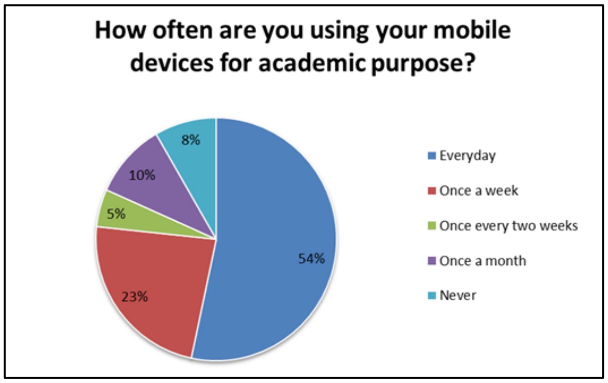

Fig. 2. Use of mobile devices for academic purposes

This survey examines the use of mobile devices for academic purposes among the university students as well as the adoption of a BYOD trend throughout the higher education. A single choice closed question will be asked about how often the participants on using mobile devices for academic purposes. Based on the survey result as shown in Fig. 2, there are 32 participants (54%) use their mobile devices for academic purposes every day, 14 participants (23%) use their mobile devices once a week, 3 participants (5%) use their mobile devices once every two weeks, 6 participants (10%) use their mobile devices once a month and 5 participants (8%) not using their mobile devices for academic purposes.

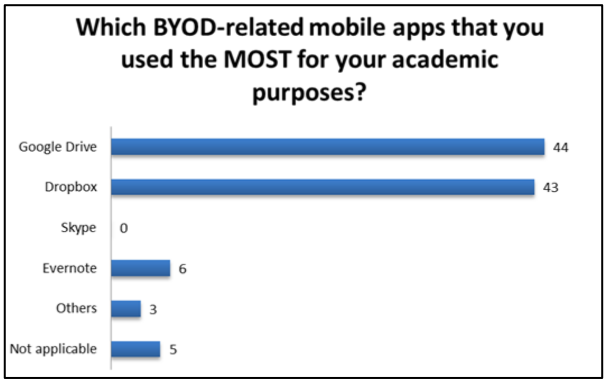

Fig. 3. Use of BYOD-related mobile apps for academic purposes

Next, a multiple choice question will be asked on which BYOD-related mobile apps that the participants used the MOST for their academic purposes. Based on the survey result from Fig. 3, there are two BYOD-related mobile apps that our participants used the most for their academic purposes: Google Drive (73%) and Dropbox (72%), followed by a note taking app, Evernote (10%) and other mobile apps such as OneNote, Notepad, WPS. Apparently, participants are not using Skype mobile app (0%) for their academic purposes. However, there are 5 participants are not using any mobile apps for their academic purposes as well.

B. *Examine the Student's Security and Privacy Awareness and Knowledge on BYOD Mobile Device and Apps*

In this survey, participants also tested on several questions that are related to the security and privacy awareness on downloading the BYOD-related mobile apps as well as their opinions on how to secure their personal mobile data after installing and using these mobile apps for their learning process. From the survey result shown in the Fig. 4, there are 58% of the participants answered that they are viewing on the reviews of the BYOD-related mobile apps before they download and install them, while the rest of the participants (42%) are not viewing on the reviews before they download and install the apps.

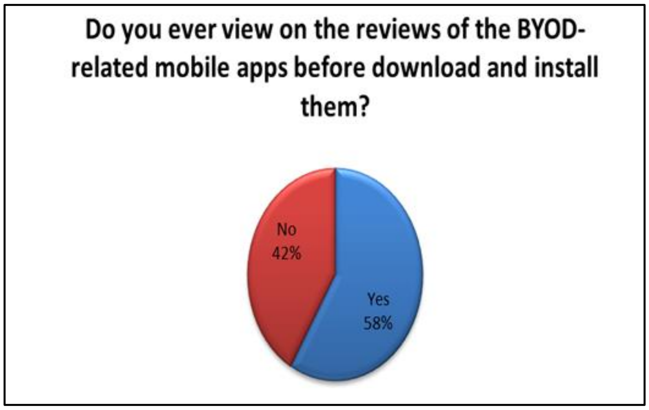

Fig. 4. View on reviews of the BYOD-related mobile apps

From the survey result shown in Fig. 5, there are 89% of participants answered that they have not read and understand the BYOD-related mobile app's "Privacy Policy" before they download and install the app, while there are only 12% of participants answered that they have read and understand the "Privacy Policy" before they download and install.

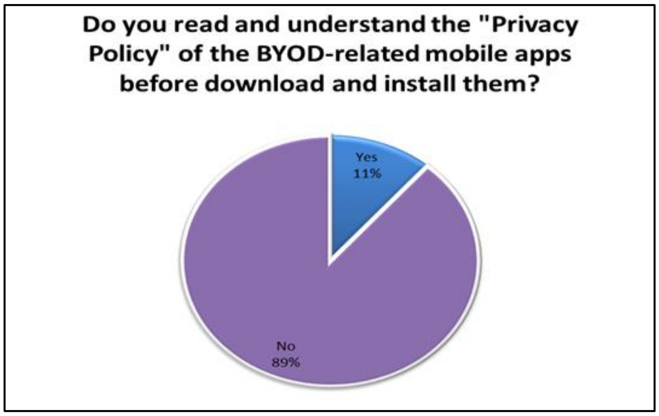

Fig. 5. View on privacy policy of the BYOD-related mobile apps

From the survey result shown in Fig. 6, there are 43% of participants answered that they have checked and read the app permissions that the BYOD-related mobile app could be accessed before they accept and install the app, while 57% of participants answered that they have not read the app permissions before they accept and install the app. So, there are still a lot of mobile users not checking on the app permissions to access sensitive information, such as mobile data, such as identity, contacts, location and device id.

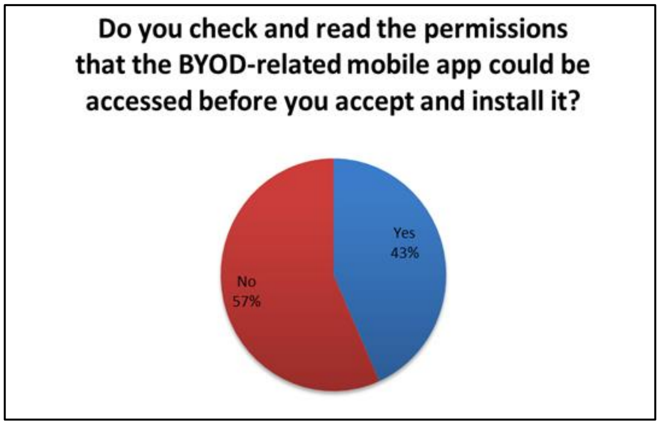

Fig. 6. Check the permissions of the BYOD-related mobile apps

For the next question, the participants are required to provide their opinions on how they feel that is it reasonable for an app to access too much personal data such as identity, contacts, location and device id through the stated app permissions before they decide to install the app. From the survey result shown in Fig. 7, almost 92% of participants answered that it is not reasonable for a mobile app to access too many personal data through the stated app permissions. Whereas, only 8% of participants answered that it is reasonable for an app in order to access these personal data by providing several reasons such as: (a) some mobile apps can be more reliable and useful once the apps accessed these personal data, (b) some mobile apps will automatically setup the app account with syncing the personal data, (c) personal data which accessed by the mobile apps will not easily expose to someone else.

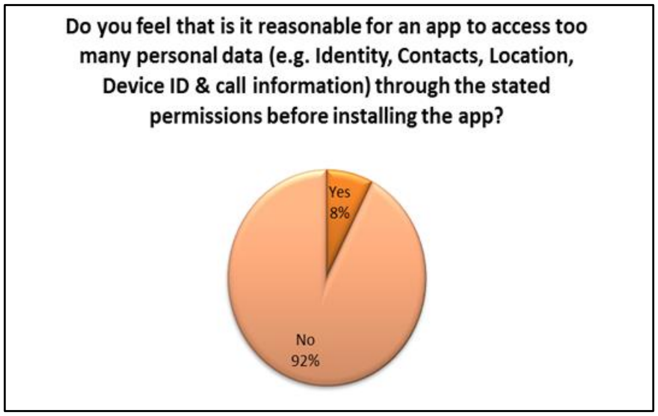

Fig. 7. Opinions on accessibility of mobile apps through permissions

From the survey result shown in Fig. 8, there are 85% of participants answered that they do not feel secure when they are signing in their BYOD-related mobile app's accounts when the app does not have any indication of SSL connection or a visible HTTPS indicator. Whereas, there are 15% of participants answered that they are feeling secure when signing in the BYOD-related mobile app's accounts even though there is no HTTPS indicator.

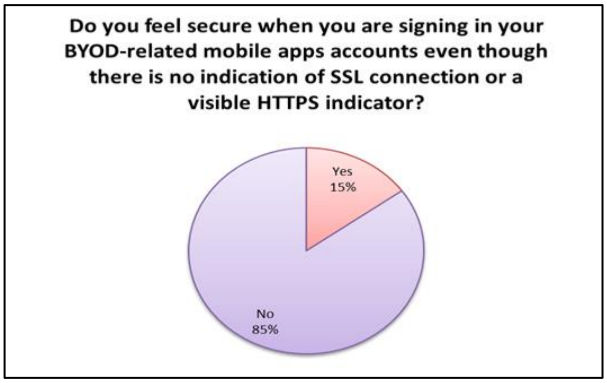

Fig. 8. Opinions on SSL connection for BYOD-related mobile apps

The reasons of some participants answered that they are feeling secure when they sign in their BYOD-related mobile app's accounts even though there is no indication of SSL connection are: (a) some of the participants believed that there have many researchers around the world focus on these mobile app security, (b) some of the participants assume that these mobile apps have a strong security since these mobile apps developed by well-known developers, (c) some participants assume these mobile apps are secured based on the stated policy, (d) mainstream mobile apps from Google or Dropbox are generally secure and there will no security issues should be worry about.

In Fig. 9, there are 83% of participants do not share their BYOD-related mobile app's personal login credential to their family or someone who close to them, whereas there are only 13% of participants are sharing their login credential to their family or people who close to them. However, only 4% of participants did not know their login credentials have been shared with someone else.

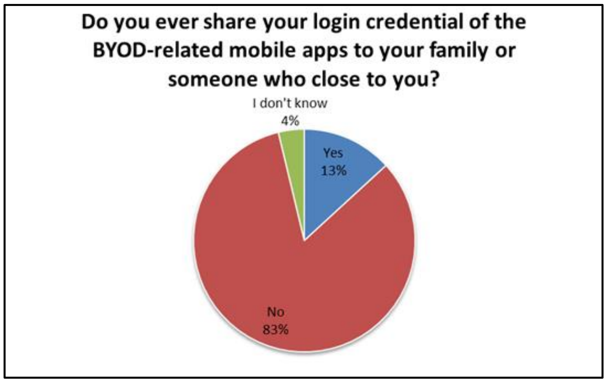

Fig. 9. Sharing login credential of the BYOD-related mobile apps

In Fig 10, nearly 38% of participants did not know the security feature of two-step verification for mobile apps, and 36% of participants did not use two-step verification for their BYOD-related mobile apps. On the other hand, 26% of participants are using two-step verification to verify their BYOD-related mobile apps.

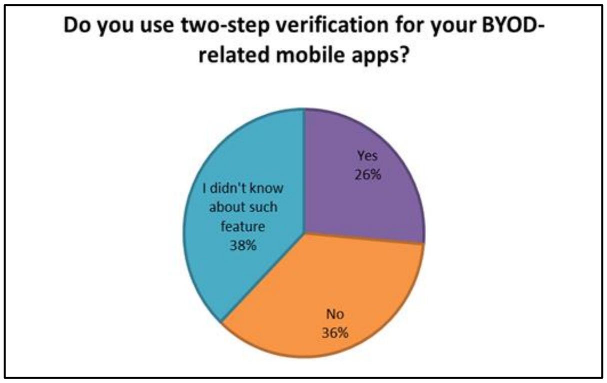

Fig. 10. Use of two-step verification for BYOD-related mobile apps

For the next question, participants will be asked for the opinion on how to create a strong and complex password for the login credentials of mobile apps. Most of the participants have provided similar answers, which is a strong and complex password can be created by the combination of capital and small letters, mixture of alphabetic, numeric and special characters/symbols, password length should be at least 8 characters, passwords should not relate to any personal information such as phone number, IC number and date of birth. Besides that, different accounts should have different passwords. Some of the participants also recommended the implementation of both password and biometric credentials.

In Fig. 11, there are 60% of participants are not syncing or sharing their personal files through BYOD-related mobile apps while accessing the public network or open area Wi-Fi. On the other hand, 40% of participants are accessing the open area Wi-Fi from any locations (ie: coffee shops and airport) when they are syncing their BYOD-related mobile apps' files.

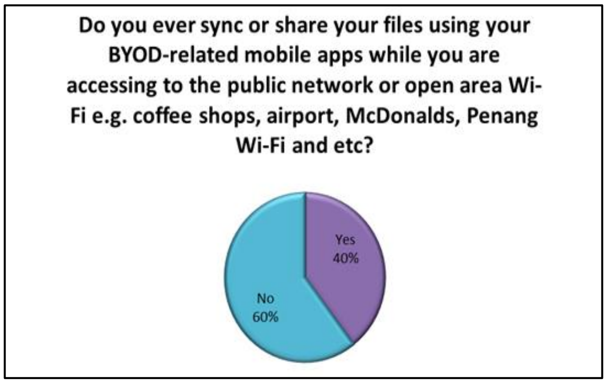

Fig. 11. Access BYOD-related mobile apps through public Wi-Fi

From the survey result shown in Fig. 12, there are nearly 60% of participants are not setting up any passcode/pin-code or add an encryption option in order to keep their personal files in a mobile encrypted and safe. Whereas, there are 34% of participants are adding passcode or encryption option to protect their valuable files on their mobile devices. In addition, there also have 6% of participants did not know the security feature of passcode or encryption option.

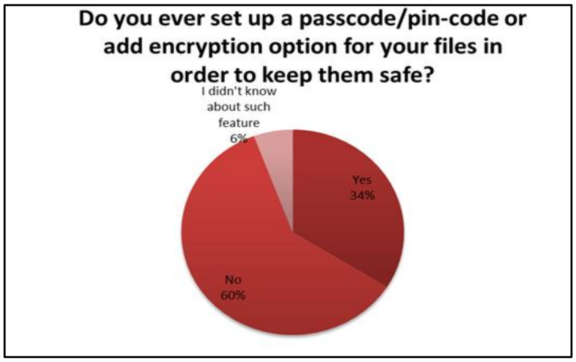

Fig. 12. Set passcode/encryption options for mobile files

Next, we will let the participants proceed to the questions related to the rating of several security and privacy concerns that will impact the mobile devices. For the security concerns, the research has listed out several concerns, such as:

- Lost or stolen mobile devices with personal data
- Malicious applications downloaded to the mobile devices
- Connected mobile devices to unsecured Wi-Fi or networks
- Accessed to insecure web browsing
- Lack of security patches on mobile apps
- High rate of users changing or upgrading their mobile devices
- Lack of efficient encryption methods on mobile apps

In the Fig. 13, for the first security concern: Lost or stolen mobile devices with personal data, where there are 33 participants or more than 50% of participants rated this security concern that can provide 100% of the impact of the security of mobile devices. For the second security concern: Malicious applications downloaded to the mobile devices, where most of the participants are rating this security concern that provides 80-100% of the impact (40 participants in total) to the security of mobile devices. Whereas for the third security concern: Connected mobile devices to unsecured Wi-Fi or networks, where the majority of the participants (20 participants) rated this security concern can provide 50% of the impact of the mobile devices.

For the fourth security concern: Accessed to insecure web browsing, where there are 19 participants (32%) rated it as it can provide 50% of the impact of the mobile devices instead of 100% of the impact of the mobile devices. The fifth security concern: Lack of security patches on mobile apps is quite similar to the fourth security concern, where there are 23 participants (38%) rated it as it can provide 50% impact of the mobile devices. On the sixth security concern: High rate of users changing or upgrading their mobile devices, where the majority of the participants (19 participants) have rated this security concern as it can provide 50% of the impact of the mobile devices. For the last security concern: Lack of efficient encryption methods on mobile apps, where the majority of the participants (24 participants) also rated this security concern as it can provide 50% of the security impact of the mobile devices.

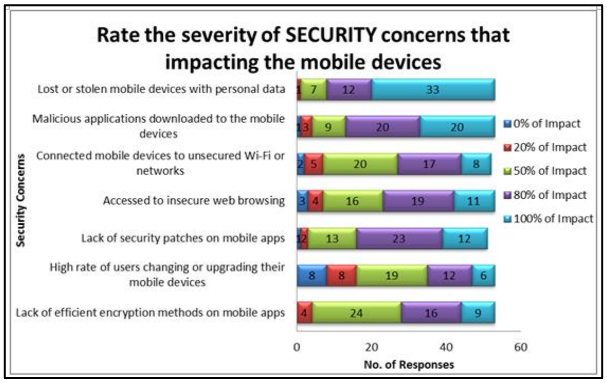

Fig. 13. Severity of security concerns that impacting mobile devices

For the privacy concerns, the research has listed out several concerns such as:

- Mobile data/information leakage
- Mobile user's location has been tracked and collected
- Collection on user identity by service providers
- Lack of transparency on mobile app permission
- Sniffing and snooping on mobile phone sensors
- Losing access of ownership of mobile data

In Fig. 14, for privacy concern, such as mobile data/information leakage, there are 29 participants rated it as it can provide 100% of the impact to the mobile devices. For the second privacy concern: Mobile user's location has been tracked and collected, there are also have 25 participants rated it, as it can provide 100% of the impact of the mobile devices. For the third privacy concern: Collection on user identity by service providers, there are 22 participants rated this privacy concern can provide 80% of the impact of the mobile devices rather than it can provide 100% of the impact of the mobile devices.

Next, for the fourth privacy concern: Lack of transparency on mobile app permission, there have a majority of 20 participants rated it as it can provide 80% of the impact rather than 100% of the impact to the mobile devices. For the fifth privacy concern: Sniffing and snooping on mobile device sensors, there has a majority of 22 participants rated this privacy concern as it can provide 80% of the impact of the mobile devices. For the last privacy concern: Losing access of ownership on mobile data, there has a majority of 21 participants rated it as it can provide 100% of the impact of the mobile devices.

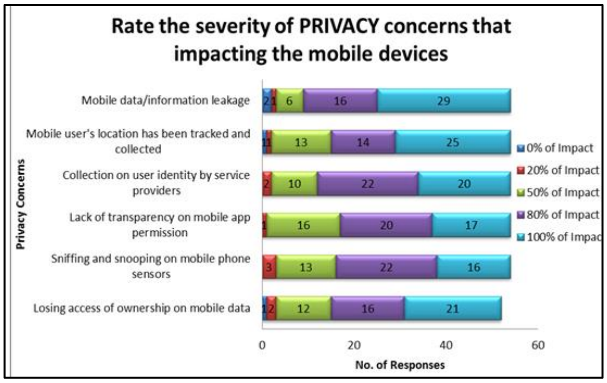

Fig. 14. Severity of privacy concerns that impacting mobile devices

In order to improve the student awareness on the security and privacy issues inherent on different types of BYOD-related mobile apps, there are a set of defined security controls such as: Authentication, Authorization, Confidentiality, Integrity, Availability and Non-Repudiation are taken into account to determine which security controls will be the most important for protecting the mobile data.

In Fig. 15, there are 67% of participants rated that Authentication is the most important security control for mobile user to protect their mobile data. Whereas, there are 23% of participants also indicated that Authentication is a very important security control which is needed for mobile devices.

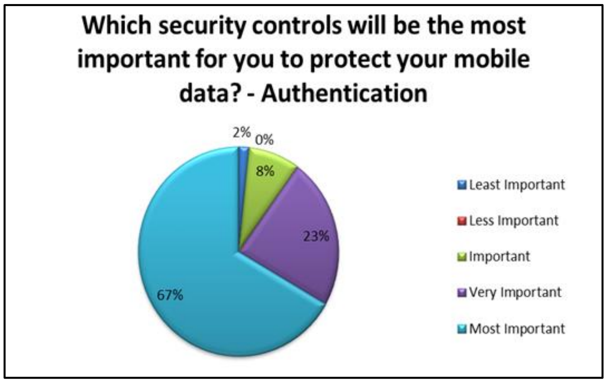

Fig. 15. Security controls for mobile data: Authentication

In Fig. 16, there are 52% of participants rated that Authorization is one of the most important security controls for mobile devices followed by 35% of participants also rated it as it is very important.

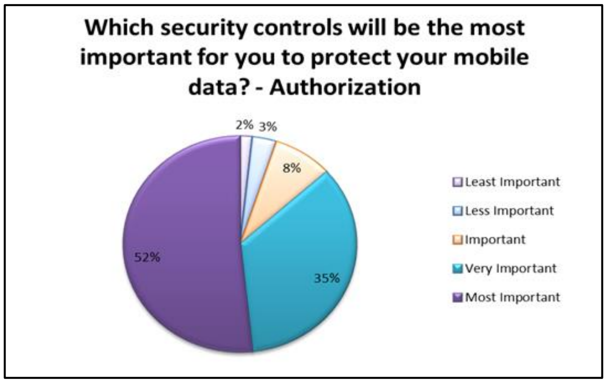

Fig. 16. Security controls for mobile data: Authorization

Similar to previous two security controls, there are more than half of participants rated the security control: Confidentiality (as shown in Fig. 17) as the most important security control for mobile devices followed by 30% of participants rated it as a very important security control.

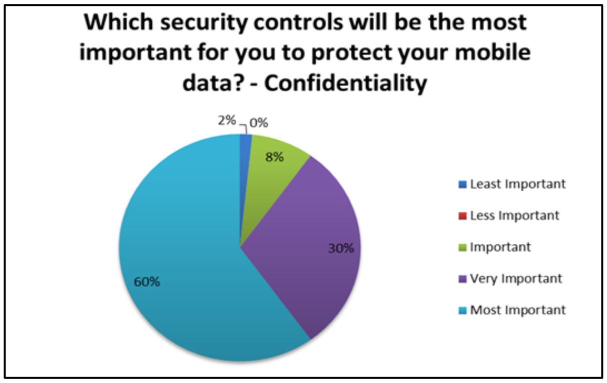

Fig. 17. Security controls for mobile data: Confidentiality

For Integrity security control (see Fig. 18), there also have 62% of participants rated this security control as the most important security control for protecting the mobile data and 30% of participants rated it as very important.

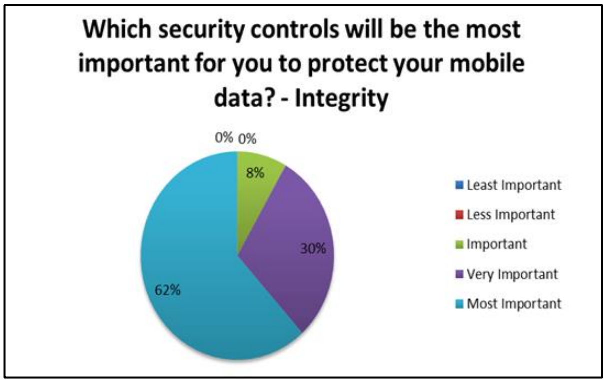

Fig. 18. Security controls for mobile data: Integrity

Unlike the previous security controls, there have only 43% of participants rated Availability (see Fig. 19) as the most important security control of mobile devices while 37% of participants rated it as very important and 20% of participants rated it as important.

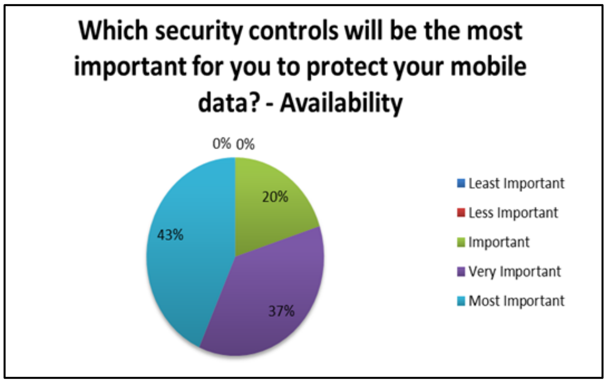

Fig. 19. Security controls for mobile data: Availability

For the last security control: Non-repudiation (see Fig. 20), there have about 55% of participants rated it as the most important security control of mobile devices and 30% of participants rated it as very important and the rest of participants rated it as important.

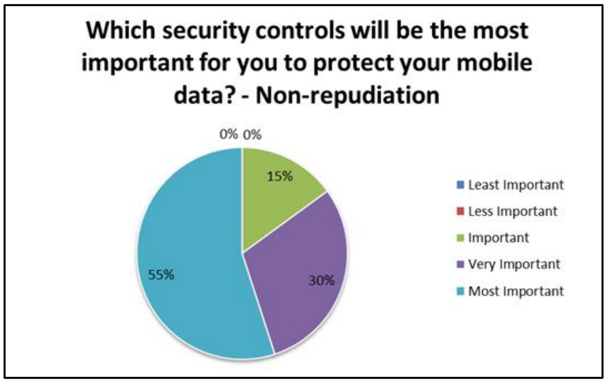

Fig. 20. Security controls for mobile data: Non-Repudiation

V. SURVEY DISCUSSIONS

Survey discussion is given in this section.

A. *Growing Trend of BYOD Higher Education*

Based on the survey results stated from Fig. 2 and Fig. 3, it could be concluded that the trend of BYOD is starting to adopt into the higher education system since there are quite a number of USM students started to use their own mobile devices for their academic purposes instead of their personal usage. Statistics have been proven that many USM students started to use some of the popular mobile applications such as Google Drive, Dropbox as their educational apps in order to use these apps throughout their student life in university.

B. *Security and Privacy Awareness on BYOD Mobile Apps*

In this survey, the participants are being tested on several questions that are related to the security and privacy awareness when downloading the BYOD-related mobile apps. Based on the survey results obtained from Fig. 4, it can be proven that there are quite a number of participants that are still considering the security and safety of downloading and installing certain mobile apps that might be harmful for their mobile devices and their personal mobile data by determining the positivity or negativity of the user reviews posted on

Google Play Store or other sources. But, Fig. 5 and Fig. 6 show that most participants are often just skipped the security precautions such as checking and reading “Privacy Policy” and app permissions before they want to download and install the mobile apps. This probably came out an assumption that most of the mobile users do not really want to spend their time on reading and understanding the policies and app permissions that written by the app developers in order to notify mobile users that what kind of data that could be collected by the app itself.

Next, Fig. 8 shows that there are quite a number of participants (85%) are aware the importance of SSL connection or a visible HTTPS indicator for signing in the mobile app’s accounts, which probably suggest that many participants take the security of their mobile app’s account seriously. Fig. 11 shows that most of the participants are not syncing or sharing their files stored in BYOD-related mobile apps while accessing to the public network or Wi-Fi, this indicates that many participants aware of the danger of sharing or sync any mobile data through public Wi-Fi.

Besides, Fig. 10 and Fig. 12 show that most of the participants are still did not know how to configure several security features such as two-step verification, pin codes and encryption option in order to protect their mobile data and applications. It could be concluded that mobile user education and awareness programs are needed for educating the mobile users on how to configure several basic security features for their mobile devices or applications. In addition, Fig. 9 indicates that there has a very high percentage of participants are not sharing their login credentials as well.

Based on the survey results from Fig. 13 and Fig. 14, many participants realized there are several security and privacy concerns that will probably cause a serious impact to their mobile devices. Some of these results are supported by the study of Obodoeze, et al. [30] which demonstrated the various forms of challenging security concerns, including losses of mobile devices, virus and malware attacks and etc., and also the study of Kambourakis [26] that discussed the security and the privacy challenge of m-learning. Furthermore, survey results from Fig. 15 to Fig. 20 show that most of the participants also believed that there should be a list of defined security controls such as Authentication, Authorization, Confidentiality, Integrity, Availability and Non-repudiation used to enhance the security and privacy strengths of the mobile devices or applications.

As a conclusion of this survey, it has been proven that most of the USM students have a fundamental knowledge or awareness about the security and privacy of the mobile devices or applications, which probably indicates that many students nowadays start concerning the security and privacy risks that could be happening on their mobile devices. The survey conducted here with a small focus group of students in one of the higher educational centers in Malaysia may project results and finding that is closely correlated to the samples size and background. However, to our knowledge, there is yet for a BYOD in higher education research to be done in Malaysia. Thus, the survey results and findings can be generalized as the perception of higher education students or as the viewpoint of the Y generation as a whole.

VI. Conclusion and Future Work

This research start with collecting and studying different approaches on BYOD Higher Education, M-Learning adoption within higher education institutions as well as the security and privacy vulnerabilities and attacks that will be happened on BYOD Higher Education environment in order to find out an effective solution for solving the research problem. Hence, this research moves on to conduct the survey to investigate the security and privacy awareness among university students in BYOD Higher Education. Based on the analysis of this survey, it shows that the trend of BYOD is started among the USM students as many students started to move towards the trend of BYOD where they are using mobile devices or applications for their academic tasks. Besides, the survey results have been proven that the current USM students have a basic or fundamental security and privacy awareness and knowledge on mobile devices or applications where most of the students start concerning the security and privacy controls or services in order to protect their mobile devices or data.

Besides that, the growing trend of BYOD in higher education institutions eventually creates a new form of student learning pedagogy where students able to use the mobile devices for their academic purposes anywhere and anytime. However, this also creates a great opportunity for hackers or attackers to find new attacks or vulnerabilities that could possibly exploit the students’ mobile devices and gains valuable data from them. Hence, a further research in finding new attacks or vulnerabilities on BYOD Higher Education is still necessary in order to increase the security and privacy awareness among the security specialists and university students. Besides, the existing case studies still require some additional research in order to improve the details of the case studies as well as its impacts towards the assets or systems in terms of confidentiality, integrity and availability. This could probably make the case studies more concise, detailed and easy to evaluate using a standardized security metrics framework.

References

[1] B. Alleau and J. Desemery, "Bring your own device: It’s all about employee satisfaction and productivity, not costs!," Capgemini Consulting2013.

[2] L. B. Lau, M. M. Singh, and A. Samsudin, "Trusted System modules for tackling APT via spear-phishing attack in BYOD environment," Undergradute Research Thesis, School of Computer Science, Universiti Sains Malaysia, 2015.

[3] Z. Zulkefli, M. Mahinderjit-Singh, and N. Malim, "Advanced Persistent Threat mitigation using Multi Level Security – Access Control framework," in Computational Science and Its Applications -- ICCSA 2015. vol. 9158, O. Gervasi, B. Murgante, S. Misra, M. L. Gavrilova, A. M. A. C. Rocha, C. Torre, et al., Eds., ed: Springer International Publishing, 2015, pp. 90-105.

[4] M. M. Singh, S. S. Siang, O. Y. San, N. H. A. H. Malim, and A. R. M. Shariff, "Security attacks taxonomy on Bring Your Own Devices (BYOD) Model," International Journal of Mobile Network Communications & Telematics (IJMNCT) vol. 4, pp. 1-17, October 2014 2014.

[5] R. Afreen, "Bring Your Own Device (BYOD) in higher education: Opportunities and challenges," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 3, pp. 233-236, 2014.

[6] F. A. Yu, "Mobile/smart phone use in higher education " in Southwest Decision Sciences Institute Conference, 2012, pp. 831-839.

[7] L. Johnson, S. A. Becker, M. Cummins, V. Estrada, A. Freeman, and H. Ludgate, "The NMC horizon report: 2013 higher education edition," New Media Consortium, Texas2013.

[8] H. Akour, "Determinants of mobile learning acceptance: An empirical investigation in higher education," Ph.D. thesis, Oklahoma State University, 2010.

[9] J. K. Lippincott, "A mobile future for academic libraries," Reference Services Review, vol. 38, pp. 205-213, 2010.

[10] A. Samochadin, D. Raychuk, N. Voinov, D. Ivanchenko, and I. Khmelkov, "MDM based mobile services in universities," in International Conference on Emerging of Networking, Communication and Computing Technologies (ICENCCT 2014) Co-jointed with International Conference on Emerging Trends of Computer Science with Educational Technology (ICETCSET 2014), Zurich, Switzerland, 2014, pp. 35-41.

[11] N. S. Alzaza and A. R. Yaakub, "Students' awareness and requirements of mobile learning services in the higher education environment," American Journal of Economics and Business Administration vol. 3, pp. 95-100, 2011.

[12] N. S. Alzaza and A. N. Zulkifli, "Mobile-Based Library Loan Service (MBLLS)," in Proceedings of the Rural ICT Development Conference ’07 (RICTD’07), Executive Development Centre (EDC), UUM, 2007, pp. 1-8.

[13] P. Seppälä, J. Sariola, and H. Kynäslahti, "Mobile learning in personnel training of university teachers," in Wireless and Mobile Technologies in Education, 2002. Proceedings. IEEE International Workshop on, 2002, pp. 136-139.

[14] M. Sharples, D. Corlett, and O. Westmancott, "The design and implementation of a mobile learning resource," Personal and Ubiquitous Computing, vol. 6, pp. 220-234, 2002.

[15] K.-W. Lai, F. Khaddage, and G. Knezek, "Blending student technology experiences in formal and informal learning," Journal of Computer Assisted Learning, vol. 29, pp. 414-425, 2013.

[16] Holzinger, A. Nischelwitzer, and M. Meisenberger, "Mobile phones as a challenge for m-learning: Examples for mobile interactive learning objects (milos)," in Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on, 2005, pp. 307-311.

[17] Bandara, F. Ioras, and K. Maher, "Cyber security concerns in e-learning education," 7th International Conference of Education, Research and Innovation, pp. 728-734, 2014.

[18] J. Bradley, J. Loucks, J. Macaulay, R. Medcalf, and L. Buckalew, "BYOD: A global perspective harnessing employee-led innovation (survey report)," 2012.

[19] O. Krehel. (2011). Worse than zombies: The mobile botnets are coming. Available: http://www.idt911blog.com/2011/06/worse-than-zombies-the-mobile-botnets-are-coming/

[20] X. Jiang. Security alert: New sophisticated android malware droidkungfu found in alternative chinese app markets. . Available: http://www.csc.ncsu.edu/falculty/jiang/DroidKungFu.html

[21] A., "Information Security Risk Management," 2013.

[22] S. Poremba, "5 higher education information security threats you should know before your child leaves for college," Forbes2014.

[23] D. Caroll, M. Rose, and V. Sritapan, "Mobile Security Reference Architecture," 2013.

[24] M. Potts, "The state of information security," Network Security, vol. 2012, pp. 9-11, 7// 2012.

[25] K. Paullet and J. Pinchot, "Mobile malware: coming to a smartphone near you ?," Issues in Information Systems, vol. 15, pp. 116-123, 2014.

[26] G. Kambourakis, "Security and privacy in m-learning and beyond: Challenges and state-of-the-art," International Journal of U- & E-Service, Science & Technology, vol. 6, pp. 67-84, 2013.

[27] P. Wei, L. Feng, K. J. Han, Z. Xukai, and W. Jie, "T-dominance: Prioritized defense deployment for BYOD security," in Communications and Network Security (CNS), 2013 IEEE Conference on, 2013, pp. 37-45.

[28] Pillay, H. Diaki, E. Nham, S. Senanayake, G. Tan, and S. Deshpande. (2013, Does BYOD increase risks or drive benefits? (Unpublished). Available: http://hdl.handle.net/11343/33345

[29] S. Ismail, S. B. A. Rahman, N. M. Noordin, S. M. S. Mustafa, Z. F. Zamzuri, M. Manaf, et al., "Student perception on security requirement of e-learning services," Procedia - Social and Behavioral Sciences in 6th International Conference on University Learning and Teaching (InCULT 2012), vol. 90, pp. 923-930, 2013/10/10 2013.

[30] F. C. Obodoeze, F. A. Okoye, C. N. Mba, S. C. Asogwa, and F. E. Ozioko, "A holistic mobile security framework for nigeria," International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 2, pp. 5-11, 2013.