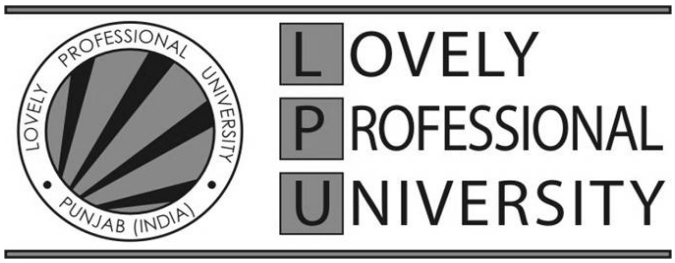


BYOD- Bring Your Own Device

Report Submitted
By

Aniket Krishna (11108949)

To

School of Computer Applications

In partial fulfillment of the Requirement for
the Award of the Degree
Of
Master of Computer Applications
Under the guidance
Of

Mr. Sukanta Ghosh
March 2017

DECLARATION

I hereby declare that the pre-dissertation report entitled "BYOD- Bring Your Own Device" submitted for the MCA degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

DATE:

Aniket Krishna
(11108949)

CERTIFICATE

This is to certify that Aniket Krishna has completed MCA dissertation report titled BYOD-Bring Your Own Device under my guidance and supervision. To the best of my knowledge, the present work is the result of their original investigation and study.
No part of the pre-dissertation report has ever been submitted for any other degree or diploma.

The dissertation report is fit for the submission and the partial fulfillment of the conditions for the award of Master of Computer Applications.

Date:

Signature of Mentor
Name: Sukanta Ghosh
UID : 19539

ACKNOWLEDGEMENT

While the rest of the research is meant to convey the technical work done, this is the only place to take the liberty to express personal gratitude. No one can even survive: let alone building a research dissertation, without countless direct and indirect helps from others. First and foremost I would like to place on record my deep sense of gratitude to Mr.Sukanta Ghosh, Assistant Professor, School of Computer Applications, Lovely Professional University, Punjab, India, for his generous guidance help and useful suggestions.

I am also grateful to the persons who have invested their precious time by providing their insights in the survey for data collection.

By concluding, I would like to take this opportunity to thank all my friends for reminding me that there are many other important things in life than studying.

TABLE OF CONTENTS

LIST OF FIGURES

IDENTIFICATION AREA

This paper researches on the BYOD- Bring your own device, refers to the policy of allowing staff to bring in person in hand mobile devices (laptops, tablets, and sensible phones) to their work and to use those devices to access privileged company data and applications.

In the following review of the papers, I get the clear view that how BYOD can be applicable, where it can be, merits and demerits, infrastructure to be used for different conditions of BYOD and other vital things.

INTRODUCTION

In recent years there has been an expansion of technology that led to the "Consumerization of IT". People likely to work on their own devices as compare to console or devices provide by their organization, so the rise of the BYOD takes place.

The introduction of devices like the Apple iPhone and iPad, Google smartphones and tablets, and lower-cost laptops has exaggerated consumers‟ appetence for the newest technology, and that they crave that very same technology within the geographic point. IT departments generally lag behind the technology curve thanks to the trouble to check new technologies, and expense of procuring them, and also the depreciation of assets that leads workers members have taken it upon themselves to herald their own instrumentality. This has resulted within the Bring Your Own Device (BYOD) trend seen across many industries and organizations nowadays.

The reason for the rise of BYOD is the working dependence of the workers on their devices as compare to devices or systems they have been provided by their organizations. They work more effectively with their devices which led to the more production also and their own devices are also in heavier configuration as compare to the organizations provided devices, so efficient working from the workers is profitable for the organization at many levels. It is cost saving with more productivity and hence many companies and organizations permitted the BYOD (at some level).

In 2012, the U.S.A-Equal Employment Opportunity Commission adopted a BYOD policy but many employees continued to use their government-issued BlackBerrys just because of concerns about billing and the lack of alternative devices.

Several problems and solutions are associated with the BYOD adaptation as the proper security services, implementation at several levels which may come up with the change in installed infrastructure and Cloud computing.

LITERATURE REVIEW

Scott Emery et.al (2012) the paper describes the term "Consumerization of IT" that changes the ways in which the IT departments must plan for the management of technology. It describes the factors needed to be considered by the IT leaders in higher education for developing an institution to support the handheld devices- basically BYOD strategy.

Further, it defines the several problems related to BYOD strategy although they are easier to use, more convenient and allow employees to mix their personal work and work- related information. It addresses the security of the information that includes the unauthorized access of the sensitive data of the organization or any other related information that may be stored on the device or on the organization's network and could be the malicious attack.

The policy development for the BYOD which may include the several factors that how to manage the system. The use for the authorized and unauthorized person followed by the policy violation and policy review (need for some changes) and limitation of the person or any other member the liability. At the organizational level how the BYOD policy and data security can be implemented at the same level of the user education and mobile learning credibility that how they can personalize their privacy settings with personal information and keeping the strong passwords for disallowing the further intrusions.

The given stats from IDC (international Data Corporation) and Gartner for the sales of smartphones and tablets which are hitting in million counts and are much convenient that the systems provided by the organization to work- making the employee work on their devices only.

For the organizations- promoting the BYOD policy is also the cost saving as well as the productive and competitive advantage for them. So many started implementations and some are still working with this policy by minimizing threats they had with the policy at some level to increase the production.

Tim Slottow et.al (2012) this paper directs to the recommendation to the BYOD as per suitability, governance, IT support, security, training, and awareness. The level at which how much the BYOD is suitable for the organization and is needed by the employees followed by the governance as the policies need to be settled for the running strategy. IT supports is very much needed for the implementation as well as the proper working for the devices which needed to operate inside the new working environment. IT support also played the crucial role in security for the any unidentified happening in the environment after the BYOD introduction furthermore relating to the organization's data security. Training and Awareness for the employees that how they can use their devices with maximum security and also depends on IT services that how much privileges they have been got to go through the personal data. How they need to share their information and with whom- all need to let them know. Awareness about their credentials that is provided by the organization- needed to be used effectively in a safe manner to avoid any mistake which led to a severe problem.

Currently, the IT services like VPN (virtual private Network) for the connection only inside the organization as well as the wireless network are implemented at some level for the working environment of employee's owned devices.

BYOD comes with the benefit mainly the employee satisfaction, increased productivity and cost saving.

The risk with the BYOD mainly in 3 categories: Security- which related to the data security can have unauthorized access and can be misused and, HR as workers work after working hour but didn't pay as they working overtime for office task and Financial which covers the change in infrastructure, security cost and supports. BYOD helps in the risk mitigation as this trend highlighted (and can be the highlight) the several risks already present in an environment- giving the opportunity to minimize them.

The flexibility of BYOD combined with lean modern next generation technology services and a modest set of risk-based controls will help us achieve the organization as well as individual's goal.

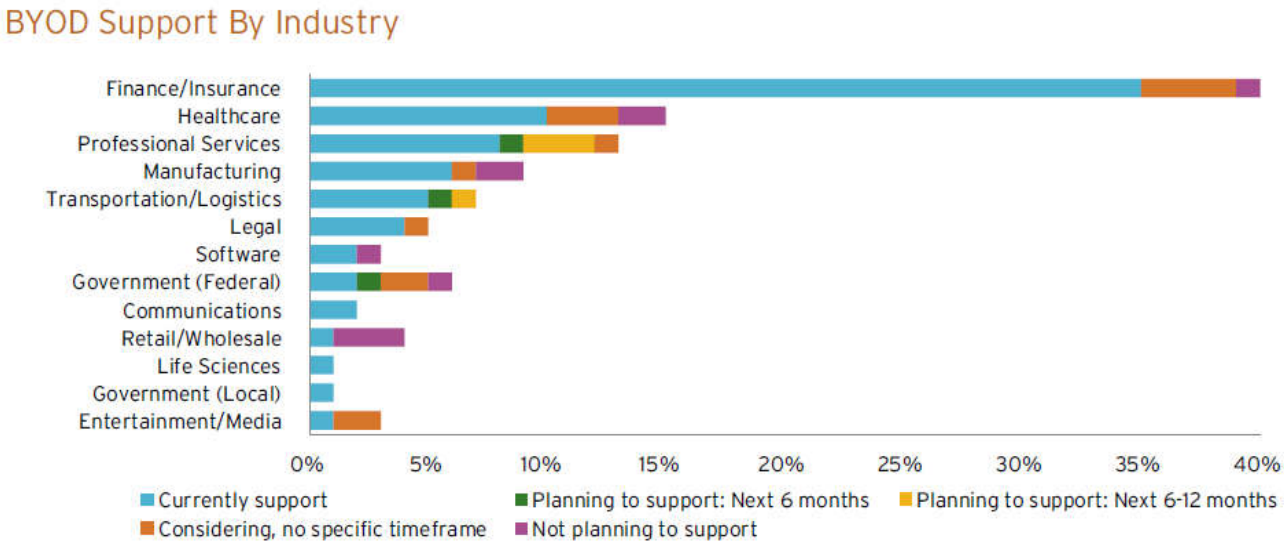
Robert J. Mavretich et. al (2012), this paper account for evolving legal environment that assumes export of the corporate as well as customer data outside the corporate network borders and protection. In it, potential ways in which an organization can provide what employee demand in BYOD program to increase productivity, as well as mitigating the legal risks that this program introduced in the working environment.

This paper talks about the concept of "consent"- that is agreed to some specific parameters according to which something can be done with the information. The continuing change of generational wave, high-level legal risks are considered- Maintaining and storing corporate data on personal devices, Incident Response/Breach notification.

In the paper, the proposed solution for the maintaining and storing corporate data on personal devices is to track them that at which level they are accessed and by whom. As devices are connected in some VPN or wireless network- monitoring can be done for the connected devices so that tracking can be done in a proper way and hence data is more secure.
Incident Response or Breach notification is the security services that the information is been using by devices is related or not. Either it is personal or corporate information relativity need to be check for the particular accessing devices so that if not mention in authorized list, notification for the irregular breach can be there to aware of the threat.

Aala Santhosh Reddy et. al (2012), this paper tell about more benefits of BYOD with some related stats which are:-

1) Worker mobility.
2) Improved employee satisfaction
3) Lower cost technology adoption
4) Attracting, supporting and retaining the new talent.
5) Improved collaboration
6) Workplace transformation



The BYOD implementation challenges are also explained there which covers-

- ➔ Protecting data- For the organizations tracking lost personal devices and wiping sensitive corporate data stored on them is a major challenge.
- ➔ Security- there is no total security to keep eye on everything like attacks as well as transactions (or it is there but not implemented yet) still need to think in a different way for that.
- ➔ Support- lacking by the different resources either in implementation or the employee's support for the organizational work at that level.
- ➔ Cost- Though BYOD is cost saving but some time organizations run on unnecessary BYOD outlays like processing the related expense report and customizing apps to run on different platforms for heterogeneous devices.

To overcome from the BYOD barriers, infrastructure provisioning is proposed which covers the virtualization, encryption, and containerization of the data so that some different access mechanism can be there and hence it can play simple.

BYOD policies and strategy needs to be implemented precisely as strategy defines the roles of the employee in the organization and how their owned devices are related to using at work time. A flexible option should be always there which is scalable and better accommodate the growing demand of the BOYD.

While implementing the policies of the BYOD (which is only possible with strategies), organization need to understand and define the factors that which kind of device need to be

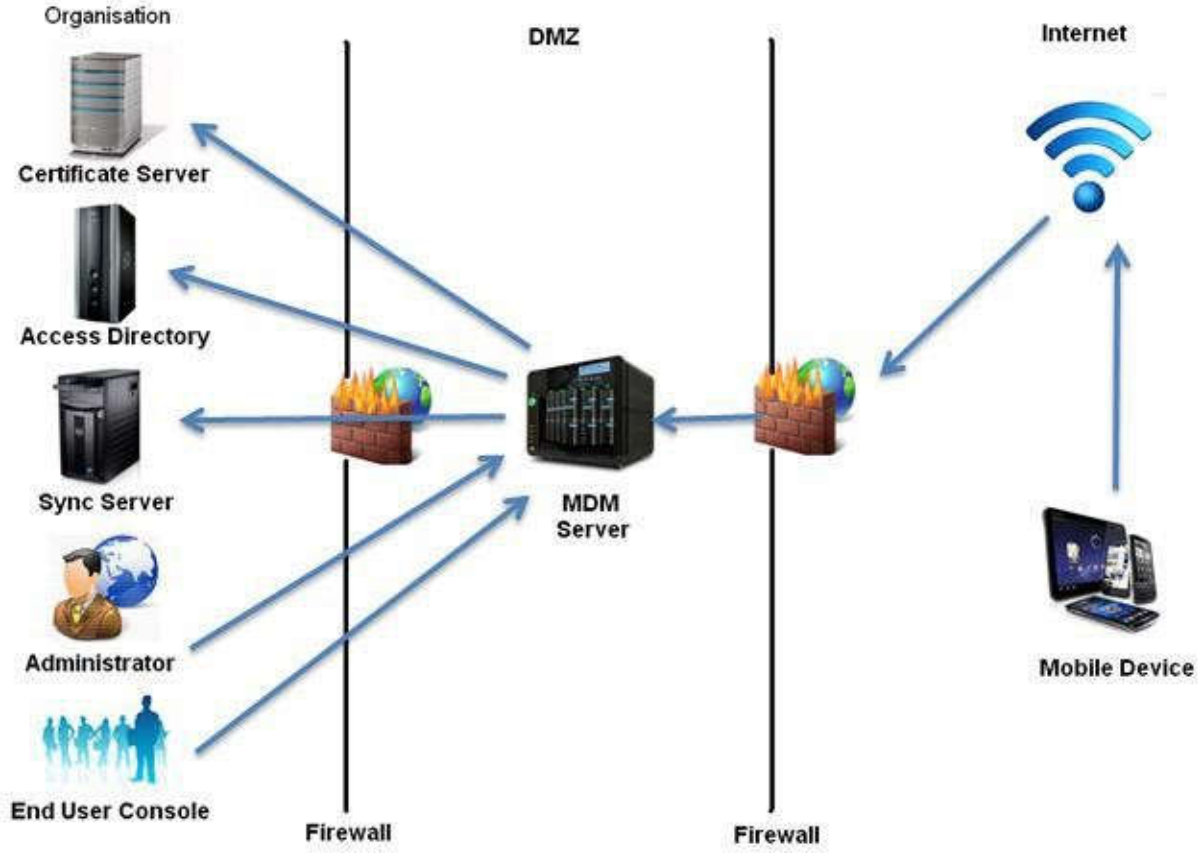
used with which operating system, the level at which risk tolerance can be done, the privacy of the employee should not be disturbed and security needed to the different – different of employee part and its position in the environment. Criteria must be there for the device and must be followed by the workers. They must be working as secure services and should be scalable so that in any case, directly the problem can be handled.

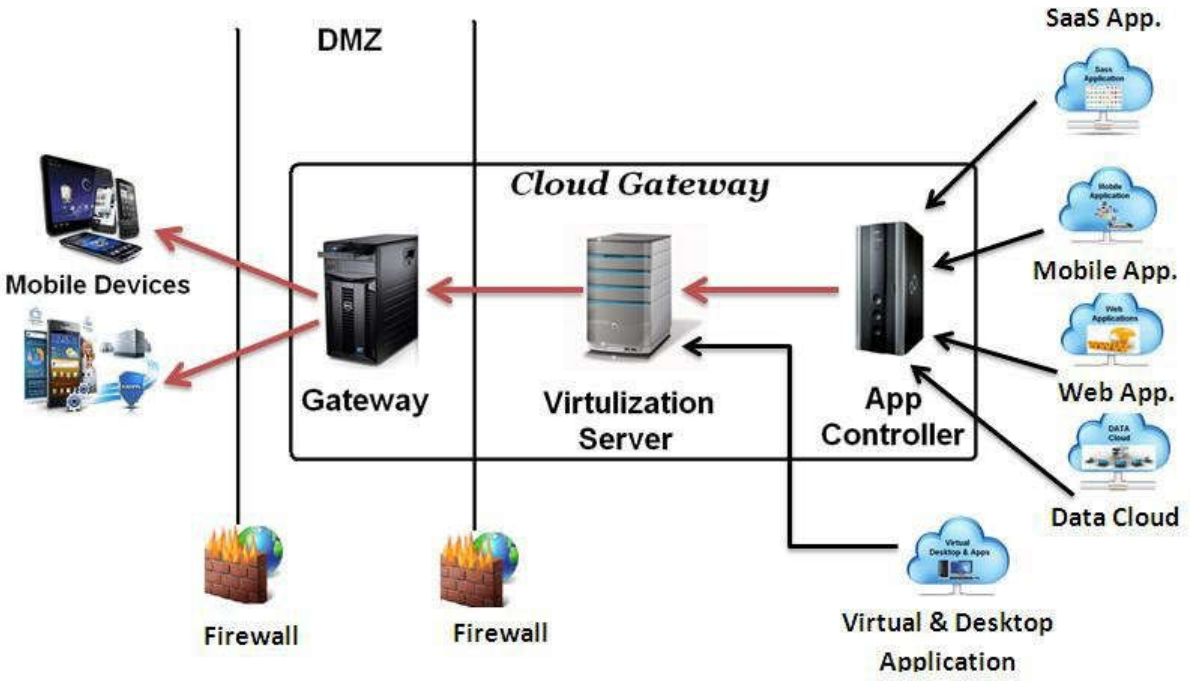
Arnab Ghosh et. al (2013), this paper defines the security risk and mitigating strategies. The risks associated with the BYOD are genuine and defined: -
Credential Information- which can be accessible by other people if the device is lost or stolen.
Confidential Business Data- secret and important data like mail, report files, documents can have unauthorized access if the device is compromised.
Phone and data Services- As eavesdropping on call and sniffing of the packets so that the device can get unauthorized access and can be rooted or jailbroken like IPhone and Smartphones of Google.

Bluetooth and Wi-Fi come as the threats as through this device can be infected. Furthermore adding to Malware attack, Spam, and Phishing.

For the mitigation of risk in BYOD environment, a mobile strategy should be there in an environment which covers up the enterprise control as well as employee satisfaction. Determining the roles and responsibilities for securing and managing of the device i.e. there should be a central administration for that. Registry and inventory of mobile devices, testing of applications which needed to installed in the devices, efficiently configuring the security services as per user profiles followed by the proper updating in security policies, patches, and settings.
The control objective is being defined for the BYOD which are: -
1) Access control and Identification
2) Security of Application
3) Integrity control
4) Data Protection
5) Compliance

The mobile device management tool helps the organization to fully control the devices supported by the API"s of the devices through which organization can lock down the devices, enforce the policies on the devices, can encrypt and wiping out the data on the devices either locally or remotely.





David Rivera et .al (2013), analysis the different security controls which are mobile Application control, Enterprise Sandboxing and Cloud Computing Management

Mobile application control is uniquely for the device recognition and certain authorization is done for the use of it so the device can be uniquely traced.

At back, a further implementation is done to control the flow of information between remote server and device so that if malware attack is done it cannot access the rest data from other devices.

Securing the access to the cloud by introducing identity management techniques including strong authentication and multifactor authentication is desirable.

Defining cloud classes based on the different security and trust profiles a cloud service provider may enforce. This classification will help to distribute assets between distinct cloud providers considering the appropriate level of security required by this specific asset.

RESEARCH GAP

The implementation of BYOD policy is easy at a small level but to rationalize the problem which occurs in at big level cannot be avoided. As a whole, to concern with the security aspects- at the vast level it can be implemented but the risk will be always there to data. Since several implementations at small level can mitigate the risk up to some level but it is difficult to say that at big level –supposing in any organization whole BYOD policy implementation is higher intensity risk of which didn't comes out with much mitigation.

The other implemented work are lacking behind in some aspects each time as considering the every factor of the probable risk is too tough. Every time things needed to change according to the related policy which always increases the security risk to the organization data as well as in related circle also.

I can see that implemented BYOD policies are limited to some aspects only as their implementation is done but seems like only done for the employee satisfaction, ease of use and working with own devices which also increases the productivity. Still fear of losing data of organization not allowing the employees to access the data from outside.

The Device configuration also threats sometimes so the implemented BYOD policies also limited to some device only so that employee could use its own device but still need to be the specific ones that are been allowed by the organizations.

PROPOSED RESEARCH OBJECTIVE

The objective of the dissertation is to find out the different benefits and as work is done for the implementation of the BYOD so that it can be implemented for the university (for the students) and followings benefits are: -

1) Enterprise Mobility – Productivity affected by the student's work done as well as faculty. The BYOD policy lets the employees work in their own way without restricting them only on the organization provided devices. Their work rate will be measured according to that and so does the change also.

2) Determining the USER restriction level: - Restrictions are always there as the BYOD policy lets the employees work in there the way. In the case of students, I will propose the level of access to them in between study hours.

3) Flexibility- Data accessing from other places and way of access to them will be defined in order to reduce the Workload

4) Lowering cost: - No need to spend on the systems for students as devices are only carried by them only.

5) Data sharing between the employees and with organization got new level so that access is not limited only to the organization.

6) Pros and Cons to that and related to implementation.

This will help in future to understand to understand the different types of users behavior and comparison of user behavior can be done.

RESEARCH STUDY METHODOLOGY

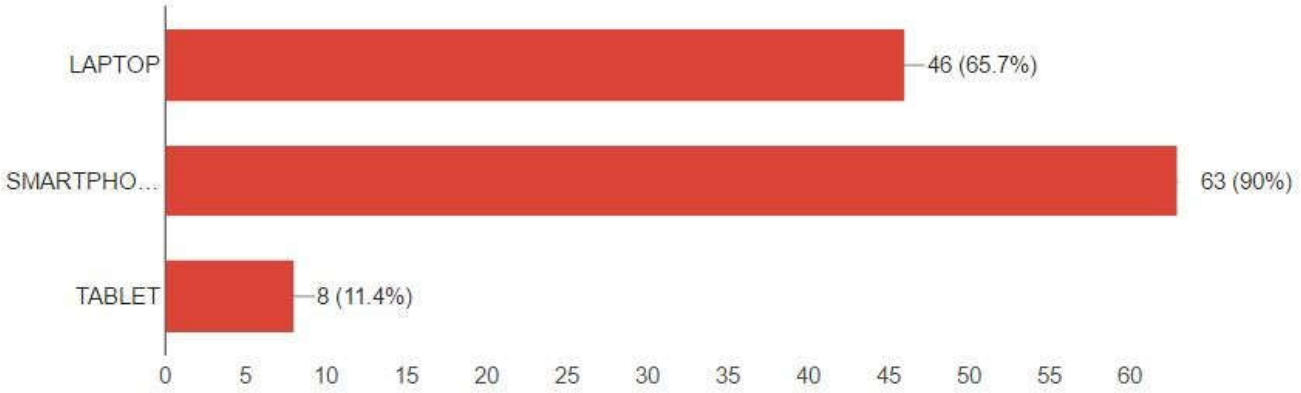
As per the research objective, I were required to design a BYOD policy for the students in the university who are officially not allowed to use their devices for their study purpose in the a and still bringing their devices to support themselves. I have done a survey of more than 100 students to know the necessity of the students as if the BYOD policy is officially implemented for them how they want it to be implemented? The Survey consists the questions from „desire to use their devices in university and actually the use of their devices in the university" to „limit up to where they want to".

The implementation is easy at a small level but a risk is always associated with it. Maybe at this small level where only students need to follow this policy is reducing the chances of risk factors but I cannot neglect the minimum risk also which is associated with the policy while implementing. As implementing the BYOD policy- some factors need to define and understand like as privacy concern, security requirements based on student's role and the risk level they are willing to tolerate. I tried to include all these in our survey so according to questions and response I got from the students - BYOD policy for the student can be design and implemented at the basic level.

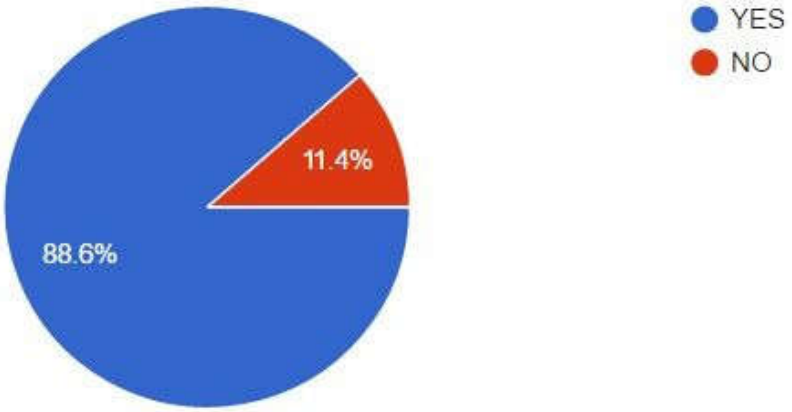
I give the questions in the survey on the basis of selection between the given options, rating on the scale of 1-10 and I welcomed their answers provided in our survey so that for the future aspects I can work on it.

The stats of the survey's question is displayed in the table which shows that if the policy for the student is implemented at starting the level- what minimum requirements are there as per their side needed, where I need to give more attention so that successfully it can be implemented and profitable to everyone. Not only on the basis of a survey I just need to implement it but also attention needs to paid to the risk associated with that and mitigation of risk needed in that case only.

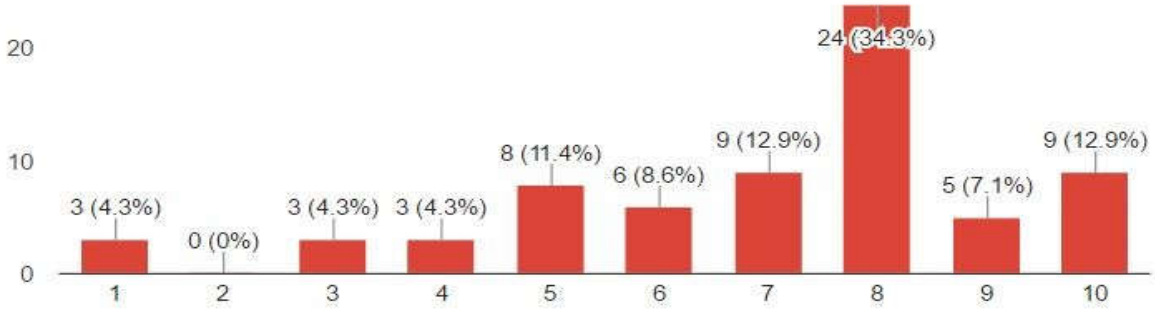
1. Select Your Device from The list You Own(selection can be more than one).
(70 responses)



2. Are you currently bringing this device(s) to university? (70 responses)

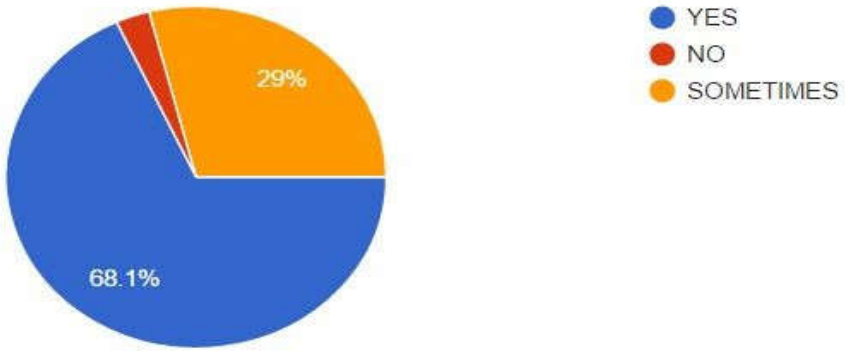


3. How often you use your device for your Study purpose Inside University Only. Rate all of them on the scale of 0-10.
(70 responses)



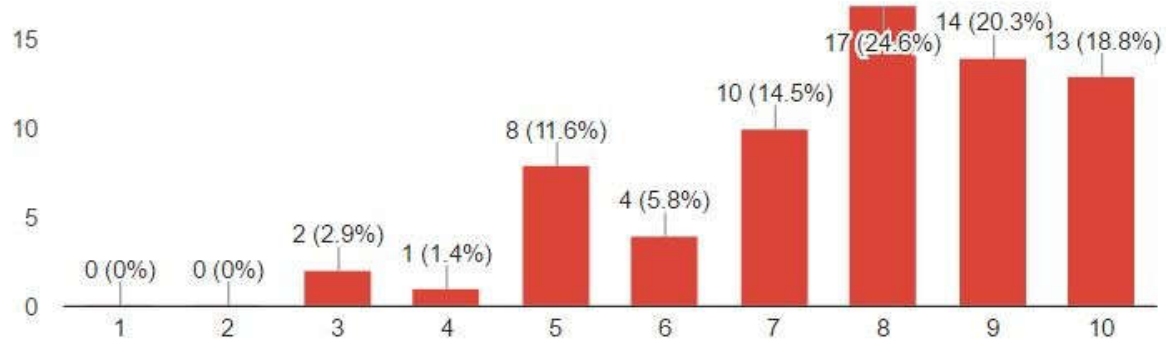
4. Do you use your device to complete homework or other assignments outside of university?

(69 responses)



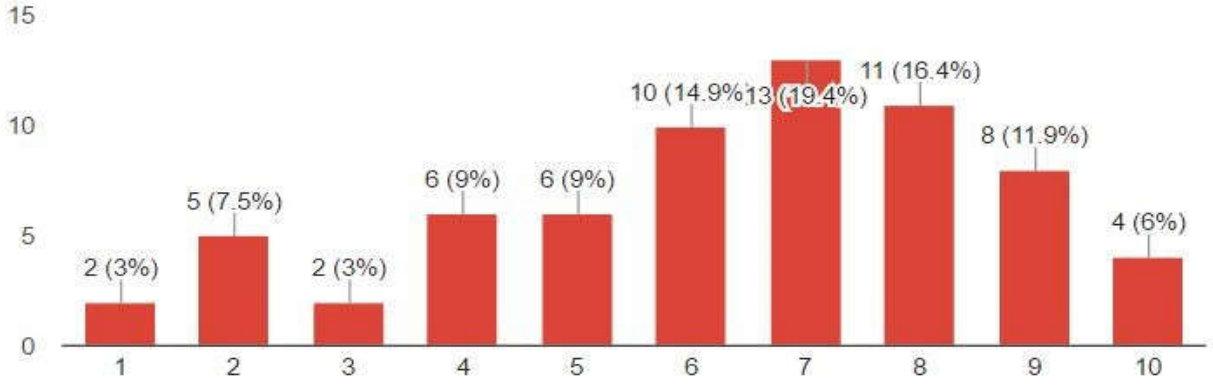
5. On average, how often the technology(could be any device like laptop, projector, tablets etc. or other utility) is use in class for study(including labs and their evaluations)?. Rate on the Scale of 0-10.

(69 responses)

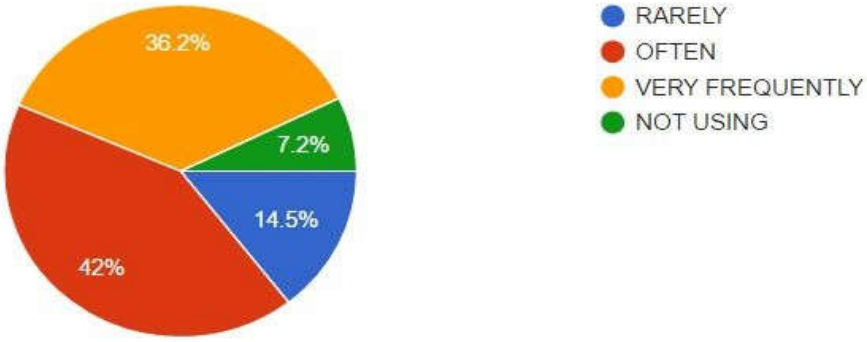


6. How often have you use a Word Processor,Spread sheet in your classes (including labs)? Rate on Scale of 1 to 10.

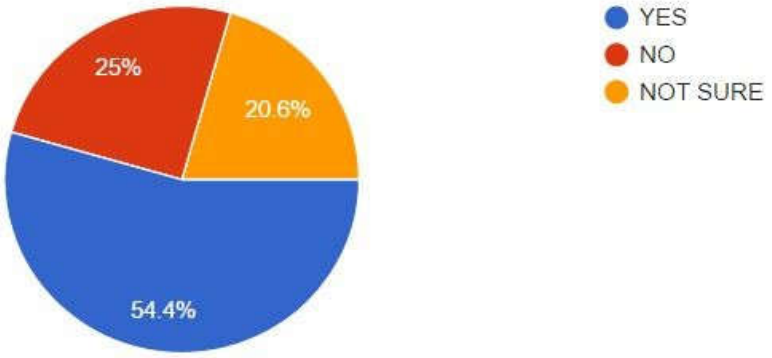
(67 responses)



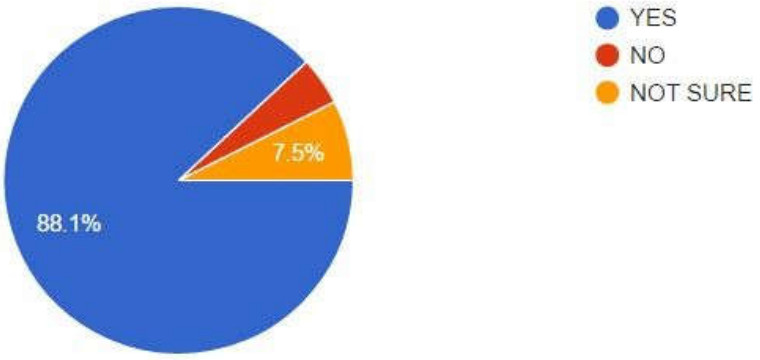
7. How often have you use technology (your device or anything) to support a presentation or project or assignments or any other in your classes and labs?
(69 responses)



8. Are You Satisfied by the devices (desktops)provided you for your lab study and evaluations? (ANSWER ACCORDING TO PERFORMANCE,WORKING AND HOW MUCH THEY ARE BENEFICIAL)
(68 responses)

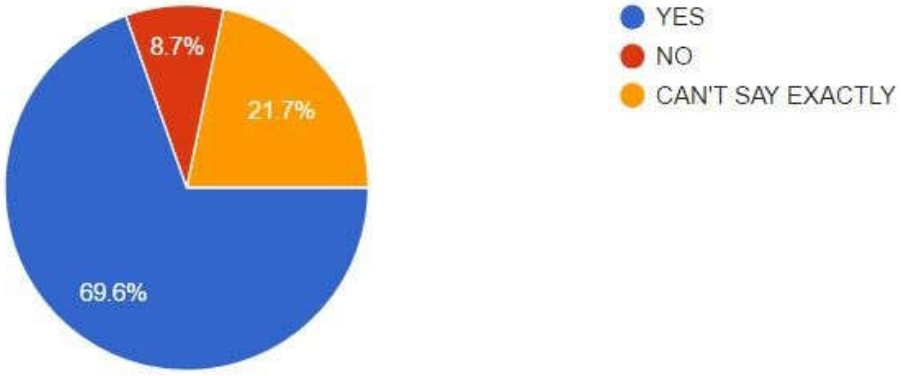


9. Do you Think Students should be allow to bring their devices to university and to use them in classes for study.
(67 responses)



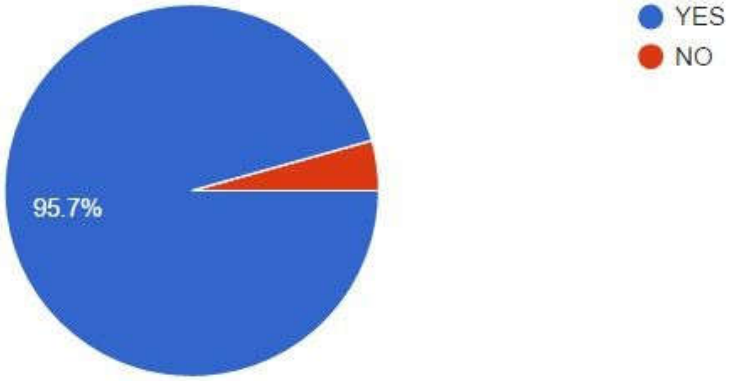
10. Does Bringing Your Own Device will solve the problems faced by you with the university provided desktop (if any problem faced)?

(69 responses)



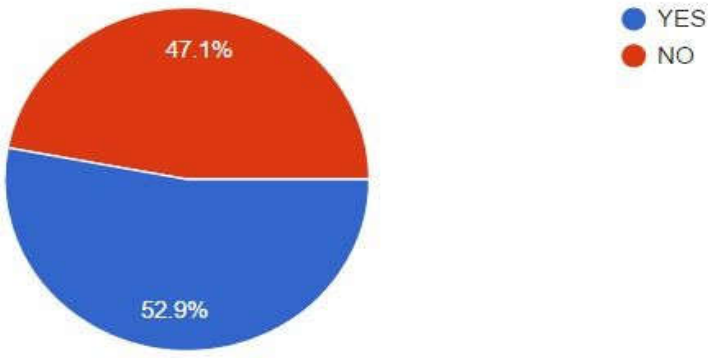
11. You Want Internet accessibility to your own device from university"s Internet?

(69 responses)



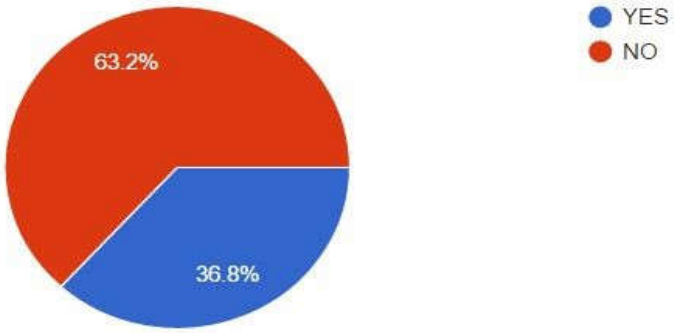
12. Do You want some restriction over internet usage on your device by university so that you cannot misuse it?

(68 responses)



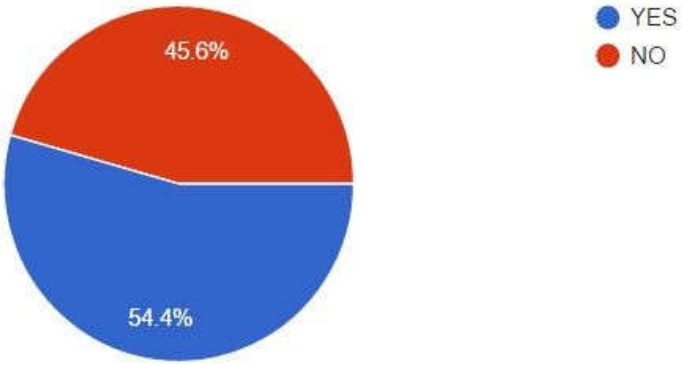
13. Don"t you think allowing you Internet on Your Own devices will be tool for time pass and distraction in study time.

(68 responses)



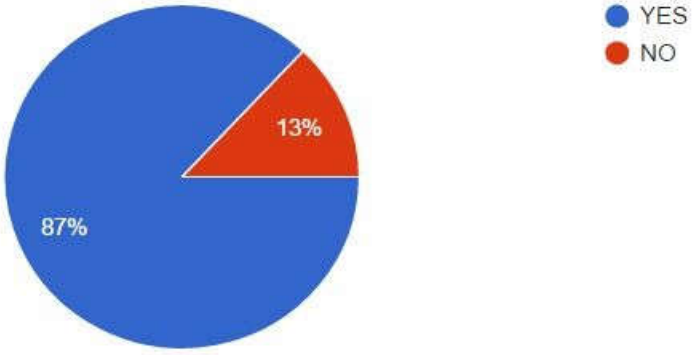
14. In order to Avoid You the misusing of your own devices, Your activity should be monitored or not?

(68 responses)



15. After implementing a better system to manage the STUDENT DEVICE(which is mitigating the risk and increases performance) overall BYOD (Bring Your Own Device) Policy should be deployed in the university officially.

(69 responses)



PROPOSED RESULT ANALYSIS

After analyzing the survey stats, I are proposing (or say designed) the BYOD policy for students at starting level - in order that they need to be implemented. I also considering the security aspects related to the implementation of this policy so that I can avoid the chances of risk.

1) First, they are permitted to bring their devices in the university officially and making them useable in classes and labs where they needed for study.

2) The internet accessibility should be given to them in order to make their study vision strong on the thing they need to at any time during their class and laboratory.

3) The permission of accessing the internet anywhere either in class or labs make them use their devices more freely but their devices will act as the medium of distraction or time pass also so I need to present the internet accessibility with some filtration also so that they cannot open any social networking sites or other for their time pass . Only study purpose site can be accessed by them only.

4) As they can use the proxies also so strong filters can be used to avoid the opening of blocked sites.

5) Downloading speed can be limited to them also if they anyhow accessed the blocked sites. In meantime, some data should be allowed to them as per their need they can download the things and accessed the sites.

6) At the time of their lab's evaluations, they should be monitored with some interface provided by the university. It can be anything either a gateway they need to go through from which only they can give their online test and lab evaluations through their devices.

7) The time they are giving their lab evaluations and online test- the interface or gateway providing by university should offers the teacher or invigilators to monitors their activity which is actually violation to the policy of anyone's privacy but at that time no other activity they can perform even their personal work so here their privacy will be restored and no threat to their data.

8) They will share their data on the local area networks but the threat will be always associated with data so they will be monitored according to their devices recognized by the university as they need to register their owned devices. In cases of any steal of one's personal data tracking can be done easily.

9) There should be different communication gateways for the teacher to student and student to teacher as every activity took place between these interfaces can be monitored differently in some local area network where each can be identified by some unique identity when connected to that local network (at the time of lab evaluations and online tests).

10) Accessing permission should be provided to teacher only so that for particular student teacher can upload or download things from that interface which will be monitoring all the time so in the case of any mistake by teacher also can be detected very easily. Student interface should consist the communication accessibility to teacher only so that student cannot be accessed the data from teacher's section.

11) The interface will automatically detect the matching timetable of student and teacher and according to that only data will be available there for the particular time or the needed time up to which they want data to be present over there like as in UMS in „Assignments Downloads" are uploaded by the teachers.

12) Authentication is needed in the interface by the student and teacher to access that interface and risk is associated to this as unauthorized access. Stealing of password will be there always in both cases of students or teachers,so after authentication there

is need of confirmation of the identity of one's by asking one private question- a very confidential one whose answer is known by the genuine user only.

13) The Devices lists are needed to update properly which are owned by the student so that if new devices tried to access the interface which is not registered in university's database- will be blocked.

14) The unique identity of a user is combined with the identity of devices owned by a student so that it can be easy to differentiate between the user owning which device and where it is using.

15) The combine identity of the student and its device will be available to the monitor by the university. So the device if using the interface for some subject at some different time from inside or outside of their local network can be detected easily as there timing for accessing the interface for the particular subject should be fixed. Moreover, to that they should not get the option to access that interface except their matching time to their timetable or as per mentioned (permitted) by the university. At the time of accessing the interface, the monitoring is needed in such a way that outside accessing of that interface can be detected which can be anything either the recognition of the device registered from student's identity or any other unique identity if device so that it can be blocked immediately.

16) IT HELP DESK should be there so that student can report to any breach if h/she feels that and avoid the inconvenience that might can happen to him/her although he/she is not involved in that case. Reporting of the problem will be more safe side to student for himself.

17) Students need to take care of their own personal data as if there any stealth or loss of data happened, he /she have backup to get that one back. Precautions they needed to take by self only.

18) If Student is lost or stolen his / her owned device, reporting should be done for that immediately, so that he/she will be free from any misuse of their owned devices.

19) The student is fully liable for the loss of device, data, and misuse in the case didn't report for the same.

20) University will have the right to take appropriate disciplinary actions in case of loss or theft of the device and not reported to authority. Any misuse of that device will be considered as the responsibility of that student and intensity of the offense will be checked starting from giving one's online test from that device to any other unethical activity.

The above-defined policy is proposed in a basic way to for the student only and can be worked officially if implemented. At this level, I tried to introduce every factor which is helpful to mitigate the risk associated with it. It is not necessary that they are existing and can be used in our defined way or can be developed but somehow, I have used in our daily life as different component and after combining them I considered them in this policy for better implementation. Risk will be always there even after implementation no one cannot be so sure about the 100% successful compilation of the security aspects but as the level increases the work in the security will also be so it is better to get implementing this as official and after use it can find out whether more improvement is needed or not.

If I go for a big level which will cover confidential data of university through the teacher, students and other authority with some different aspects and definitions.

REFERENCES

[1] Riding the wave of BYOD: developing a framework for creative pedagogies. **Authors** Thomas Cochranea, Laurent Antonczakb, Helen Keeganc and Vickel Narayana. (Received 13 April2014; nal version received 18 July 2014).

[2] Analysis of Security Controls for BYOD (Bring your own Device). **Authors:** David Rivera, Geethu George, Prathap Peter, Sahithya Muralidharan, Sumaya Khanum. (Received 13 April 2014)

[3] Emergent BYOD Security Challenges and Mitigation Strategy. Authors: Ahmed Dedeche, Fenglin Liu, Michelle Le, Saeed Lajami. (Received in 2013)

[4] Does BYOD increase risks or drive benefits? **Authors**: Ashwin Pillay Department of Information Systems, University of Melbourne Parkville, Victoria. (Received in 2013)

[5] Effectiveness of security controls in BYOD environments**. Author:** Zoran Marjanovic.

[6] BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING STRATEGIES. **Authors**: Prashant Kumar Gajar, Arnab Ghosh, and Shashikant Rai. (Received in 2013) Journal of Global Research in Computer Science

[7] BYOD And Bust. **Author**: Symantec World.(Received in 2013)

[8] Bring Your Own Device (BYOD). **Author:** Perakovik. (Received in 2012)

[9] „BYOD: Bring your own device could spell end for work PC" **Author**: Fiona Graham(Received in 2012)

[10] Factors for Consideration when Developing a Bring Your Own Device (BYOD) Strategy in Higher Education.**Author:** Scott Emery (Received in 2012).

[11] The Future of BYOD in Organizations and Higher Institution of Learning
Author: Onyechere Ugochukwu Franklin (Received in April 20150