E-ISSN: 2706-8927
P-ISSN: 2706-8919
www.allstudyjournal.com
IJAAS 2022; 4(1): 319-327
Received: 26-11-2021
Accepted: 25-12-2021

Qamaruddin Shamsi
Assistant Professor, Department of Information Technology, Kabul Education University Kabul, Afghanistan

Corresponding Author:
Qamaruddin Shamsi
Assistant Professor, Department of Information Technology, Kabul Education University Kabul, Afghanistan

Hazard investigation of Byod in Afghanistan's organization

Qamaruddin Shamsi

Abstract
Moving forward ICT administration techniques is a progressing require for nearly all organizations. At the same time, the challenges that BYOD brings to the organization need to be carefully considered. BYOD wording can allude to related concepts, advances, and methodologies that empower workers to utilize organizational assets. The utilize of distinctive databases, applications, and individual gadgets such as smartphones, portable workstations, tablets, and any other portable gadget such as memory chips and outside difficult drives can give illustrations of these assets. The execution of BYOD has brought a clear advantage to the organization. Be that as it may, the Utilize of BYOD in organizations can posture a few dangers and dangers. The most reason of this think about was to analyze BYOD dangers in Afghan organizations through cross-sectional quantitative investigate strategies. A web overview of 24 questions was conducted on different angles of BYOD hazard from different organizations in Afghanistan. Through the Utilize of crude information, overview comes about related to BYOD usage in Afghanistan have been collected. Hence, the analysts found out that IT staffs have a moo level of mindfulness of the dangers and challenges of BYOD security and the most recent advances utilized by Afghan organizations. At long last, proposals have been made.

Keywords: Bring your own device (BYOD), cyber security, information security

1. Introduction
Today, BYOD (Bring Your Own Device) has ended up a mandatory calculate for each organization to supply superior adaptability to workers, due to work and specialized necessities whereas giving representatives with diverse strategies and way better adaptability through portable gadgets. In later a long time, the field of IT BYOD has made colossal advance (French, Guo, & Shim, 2014). Of course, most organizations have actualized and exchanged to this unused innovation. BYOD lays the establishment for representatives to utilize and bring their claim computing gadgets (such as portable workstations, smartphones, tablets, capacity gadgets, etc.) to the organization and interface to the organize without utilizing the gear possessed by the organization (Koh, Oh, & Im, 2014).
In any case, security dangers within the BYOD worldview give an opportunity for programmers or assailants to discover modern assaults or vulnerabilities that might misuse representatives 'mobile gadgets and pick up critical organizational data. It has been demonstrated (Mahinderjit Singh, Wai, & Zulkefli, 2017) that fundamental security and protection information and information of versatile gadgets or applications are significant to ensuring their versatile gadgets and ensuring organizational information.
Afghanistan could be a nation that employments data and communication innovation, which is spreading quickly, and ICT plays an imperative part in all viewpoints of our lives (Republic, 2014). In any case, Afghan organizations don't have ICT security approaches for shopper hardware, and IT staff inside these organizations have a low level of understanding of BYOD hazard and security, which could be an enormous issue. This will clear the way for cyber security vulnerabilities and crevices over Afghan organizations.
Whereas there are numerous concerns around BYOD security dangers in numerous organizations in Afghanistan, BYOD has given noteworthy benefits to laborers in later a long time, and most workers are fulfilled with BYOD. Be that as it may, distinguishing BYOD-related security dangers and finding the foremost fitting arrangement to diminish these dangers postures challenges.
To decide the security risks associated with BYOD completely different organizations in Afghanistan, it is essential to survey the ICT division of this organization to get it the existing measures or arrangements with respect to BYOD.

The reason of this think about was to analyze the organizations actualizing and spreading BYOD in Afghanistan to set up solid security components to diminish BYOD-related dangers. This will offer assistance Afghan organizations define (1) different moving procedures, (2) defense components, (3) viewpoints of control, and (4) administration and administration to execute BYOD strategies.

2. Concept and Definition of BYOD

Concurring to (Koh *et al*., 2014) and (Ogie, 2016), BYOD implies a bunch of coordinates advances and procedures, where workers can interface to organizational systems and get to inside assets through inside gadgets, such as online databases or applications such as Steam memory USB smartphones, portable workstations and tablets, memory cards and versatile difficult drives. In expansion, agreeing to (Arregui, Maynard, & Ahmad, 2016), there are numerous definitions to decide the concept and meaning of BYOD

The definition states that BYOD can be Electronic and mobile communication devices or portable storage media (USB memory sticks, memory cards, portable hard drives, floppy disks) and media with the following features:

- Users can use this device for knowledge work.
- It is owned by individuals and not purchased by organizations.
- Equipment should be portable.
- May install third-party software applications on the device.
- The device must be able to connect via one of the wireless network interfaces, mobile phone networks (2G, 3G, 4G and 5G)
- The device has Wi-Fi or Bluetooth.

Numerous experts carry or have more than one sort of portable gadget in their take: one for trade utilize, and another for individual utilize. A few have more than one for another reason. All of these gadgets have passwords, settings, information sets, setups, and more. These different gadgets with distinctive setups and working frameworks will bring complexity and disarray to clients and framework companies. These days, remote innovation has ended up portion of everyone’s every day communication, and most organizations give comfort to its individuals by giving a structure that permits them to utilize their possess gadgets to put through and utilize the organization’s organize assets.

3. Related work on BYOD

For organizations, there are security concerns that permit the Utilize of client gadgets called third-party control advances past the control of the organization. This incorporates gear worked by temporary workers, commerce accomplices, and providers, as well as person computers, smartphones, and tablets (BYOD) of people, temporary workers, trade accomplices, and providers. Whereas organizations may reach understandings with representatives and third parties that require representatives and third-party gadgets to be legitimately ensured, these assertions are frequently not upheld consequently, so hazardous gadgets, contaminated with malware and / or influenced, can in the long run interface Sources of delicate organizations (Souppaya & Scarfone, 2016). Nowadays, Bring Your Claim Gadget (BYOD) has gotten to be one of the foremost prevalent models for each organization to supply portability and adaptability within the working environment. The approach of unused advances and the capabilities of day-by-day trade exercises. Besides, versatile systems are presently well coordinates with the Web (such as 3G, 4G, and LTE advances). Hence, in BYOD, individual gadgets (i.e., portable gadgets) can be utilized to extend representative fulfillment and decrease the taken a toll of organizational gear. Compared to computers and computer systems, portable gadgets are not well secured, and clients pay less consideration to overhauls and security arrangements. In this way, when workers utilize their claim portable gadgets to get to organizational information and frameworks, portable security has gotten to be a major issue in BYOD (Eslahi, Naseri, Hashim, Tahir, & Saad, 2014). Concurring to Disterer and Kleiner (Disterer & Kleiner, 2013), BYOD is the foremost noteworthy and genuine security chance. The secrecy, astuteness and genuineness of company information is debilitated. When unauthorized parties get to delicate individual data or private company data by controlling the gadget or interference information transmission, privacy is compromised. Operations performed utilizing gadgets with inadequately security undermine the astuteness of company information. When a gadget is utilized to trigger a trade exchange that cannot be clearly recognized, its genuineness is debilitated. In case a portable gadget is set up for individual and commercial BYOD get to ("twofold utilize"), whereas the company gets to company information, it must moreover secure the conclusion user's individual information (contacts, addresses, photographs, reports) to anticipate company get to from being ensured. Need of partition between the private division and the commercial sector poses a significant risk to the company.

Concurring to this work (Arregui *et al*., 2016), data related to the organization will be compromised by the establishment and utilize of malware. In this case, each organization ought to utilize a approach articulation to address this chance, and it is as it were prescribed to download the application from a trusted source. Amid the application establishment handle, clients will allow consents (such as permitting thrust notices or location-based administrations), as they will advantage, so security contemplations are set aside. Moreover, within the scholarly environment, most understudies utilize social media or social applications such as Facebook, Twitter, and YouTube. In any case, this may lead to the facilitating and spread of malware and infections such as Fierce blaze in students' individual gadgets (Mahinderjit Singh *et al*., 2017). Agreeing to (Fuentes, Álvarez, Ortega, Gonzalez-Abril, & Velasco, 2010) commonsense illustrations on portable gadgets, how Trojan steeds can take data from portable gadgets without the information of the client. Noxious clients can get to client contact data through a pre-installed Trojan. In expansion, common portable malware assaults such as Dream Droid (Mahinderjit Singh *et al*., 2017) allure clients to tap noxious web joins on their smartphone web clients and introduce malware. In expansion, BYOD is effectively assaulted by programmers, subsequently sending malevolent program through e-mail downloads or applications, hence assaulting someone's gadget. As a result, once a understudy downloads and actualizes malevolent computer program, the probability of a student’s individual data spill increments, and the aggressor introduces a back entryway to annihilate delicate data capabilities. A few portable clients intentioned turn off local OS security

highlights through procedures commonly alluded to as "jailbreaking" or "rooting". By jailbreaking or establishing on their portable gadgets, they can introduce or overhaul confined working frameworks and versatile applications by default for complimentary. In any case, jailbreaking or establishing can introduce unauthorized programs on versatile devices, which may present malware to their gadgets. This will make the client gadget defenseless to dangers. Portable gadgets can be utilized in secure a d risky environment.

When clients interface their gadget to an unsecured arrange (such as open Wi-Fi), the gadget will be turned on to get different security and security assaults, such as Wi-Fi capturing, Bluejacking, etc. For case, when programmers assault, Wi-Fi seizing can catch communication between smartphones and uncertain Wi-Fi scope. In the event that a client logs in to a particular versatile application or site, programmers can utilize the guest to get to the username Watchword. Executing BYOD in an organization not as it were gives representatives with a broader endpoint to get to organizational assets, but too empowers the dispersal of unauthorized touchy data, in this way uncovering information (Arregui *et al*., 2016). In case information is replicated to a portable gadget, control is troublesome to perform. Touchy data such as client information is ordinarily constrained to a little number of clients within the organization, be that as it may, utilizing individual gadgets can effortlessly duplicate that data and make representatives incidentally go past organizational security when they require electronic corporate assets to total errands. This operation is considered and manhandle of safe organizational assets. In general, workers ordinarily don't intentioned influence the security of an organization's data, but their activities can uncover private organizational data. Organizations must consider BYOD dangers and decide which administrations and applications can be gotten to from individual gadgets such as e-mail, calendars, contacts, and electronic archives. Since BYOD is embraced in a work environment, which permits representatives to bring their individual gadgets to the office, there's a hazard of losing worker individual information due to the simple misfortune or burglary of BYOD gadgets. Afterward, most individuals store a parcel of delicate individual and company data on versatile gadgets. There are a few actualities around the misfortune or burglary of versatile devices. About 1.3 million versatile phones are stolen every year within the UK (SYBASE, 2013). Hence, misplaced gadgets cause a part of information misfortune. Whereas huge sums of information are misplaced through stolen gadgets, in reality no activity is taken to secure company data or client information on individual gadgets. In this way, a misplaced or stolen portable gadget could be a major assault and influences BYOD security. In BYOD phrasing, the security viewpoint continuously alludes to individual information (such as individual emails, photographs, recordings, bank explanations, social security numbers, chat notes, usernames, passwords, and other prove) that are uncovered to the consideration of pariahs. In expansion, gadget area following issues are also one of the genuine security issues within the BYOD setting (Mahinderjit Singh *et al*., 2017). Whereas area following through portable gadget area administrations or GPS is valuable for finding misplaced gadgets, unlawful following can cause genuine security issues for portable clients. Since the area of the client has been recorded, versatile gadget following or area checking can posture a risk to the client, and potential offenders will screen the target client (Mahinderjit Singh *et al*., 2017). These days, numerous authentic or third-party portable applications give not as it were gadget following capacities, but moreover gadget following capacities. This moreover permits following of portable utilization behavior through introduced applications. This implies that the introduced application makes it conceivable to track chosen occasions that happen on the versatile gadget and record each activity performed by the versatile client. On the off chance that a client introduces different third-party applications, this will posture another protection risk to the client (Mahinderjit Singh *et al*., 2017).

Malevolent computer program (Malware) is called a computer program with malevolent code, which is modified to intentioned crush and / or disturb the ordinary working of other computer program, make botnets move, collect data and information from the have, devastate information, etc. In terms of "malware", it can be recognized as infections, worms, spyware, Trojan steeds, deceiving applications, etc. (By Robert Moir, 2013). There are a few programs software engineers within the world with malevolent aim. They purposely make noxious program to close down versatile gadgets, so that malevolent clients can take control of portable gadgets and indeed take users' individual data to back capacity on individual gadgets. A few malwares incorporate spyware, Trojan steeds and adware (Wu, Narang and Clarke, 2014). A sort of noxious computer program called spyware. Spyware may be a spy on computers, phones, and tablet frameworks. Spyware can collect data from a user's Web browsing history, such as SMS messages, emails, usernames and passwords, charge installments, and credit card data. In the event that the data isn't constrained, spyware can exchange the data to other clients through portable gadgets. Presently, how does spy computer program work on versatile gadgets? Spyware is comparative to a infection or disease. When a client opens an SMS message connect or e-mail connection with noxious computer program, a infection or disease may be installed. When the client introduces another program that contains spyware within the introduced program, another strategy that can introduce spyware into the versatile gadget. Since of the destructive behavior of spyware, most clients don't indeed know when the spyware is on their portable gadget. Trojan steeds will take users' individual data and open pop-up windows in notices to get individual data and information (Wu, Narang, & Clarke, 2014). Diminishing the chance of BYOD may be a way to ensure organizations organize from different dangers postured by portable gadgets and get to channels. To decrease the hazard of BYOD or portable gadgets, use Mobile Security Reference Architecture (MSRA), VPN, Mobile Device Management (MDM) (Donaldson, Siegel, Williams,

Aslam, 2015), Mobile Application Management (MAM) (Eslahi *et al*., 2014), Identity Access Management (IAM) (Carroll, Rose, & Stritapan, 2013), Mobile App Store (MAS) and Data Loss Prevention (DLP) (Carroll *et al*., 2013) development encompasses all Management methods and risk control BYOD in a different way.

4. Methodology of the study

The most reason and objective of this investigate is to discover fitting strategies for organizations in Afghanistan to decrease and control BYOD-related risks.

To accomplish the most reason and destinations of this inquire about, the analysts utilized cross-sectional quantitative information collection and investigation strategies, counting surveys with open and closed questions.

A. Data Collection

Primary data gathered through distribution of a simple web-based questionnaire with 24 closed ended and open-ended questions to preselected target group of IT professional from different organizations in Afghanistan.

B. Questionnaire Reliability and Validity

The unwavering quality and legitimacy of the questionaries' is accomplished through a pilot testing. The analyst focused on a bunch of five members and dispersed the survey to them; thus, after analyzing the reactions, the most targets and comes about of the Consider were accomplished. Moreover, to conduct a solid and exact study obtain important information, a few sessions and gatherings were held with IT specialists of diverse organizations. These endeavors had impressive impacts on the unwavering quality and legitimacy of the Ponder.

C. Research Design

The research objectives, research questions, research methodology and questionnaire were developed which are discussed earlier. The secondary data gathered from different sources (such as official statements, papers submitted, Books, and journals). In addition to above, for collecting primary data, an online survey with 24 questions conducted and the data analyzed by SPSS application. As the result of findings related to implementation of BYOD in Afghanistan, are collected and concrete recommendations and suggestions provided. The research process is shown in the following figure 1.

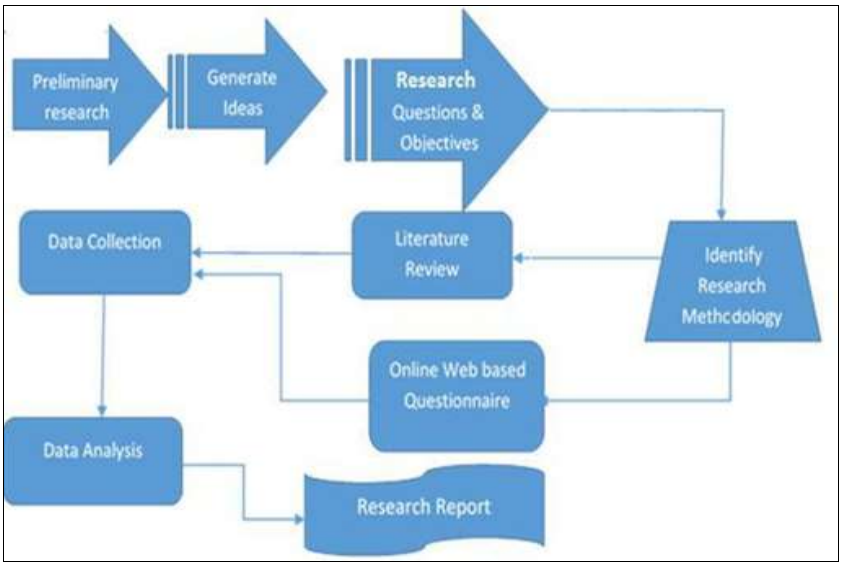

Fig 1: Research Design

5. Analysis and Result

A. Type of Organization in This Study

The result of the study gives data around the sorts of organizations where respondents are working. As per underneath figure, two-fourth of the respondents are working with administrative organizations, be that as it may the remaining respondents are have a place to national both non-governmental and private division and universal organizations.

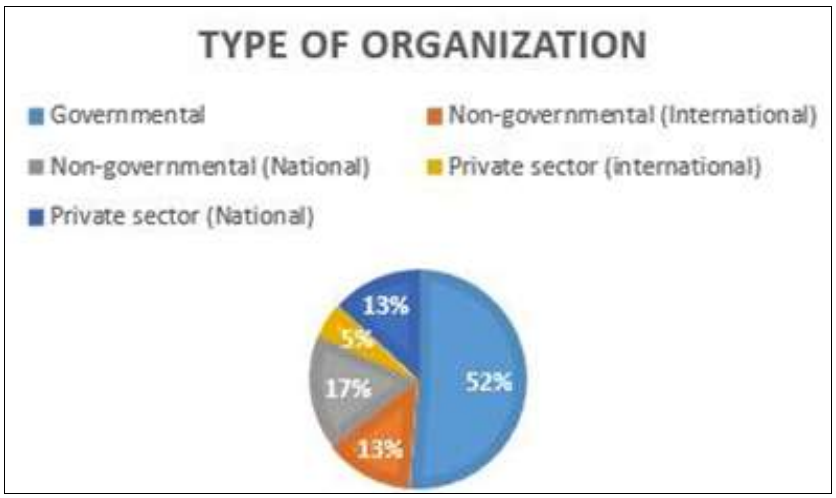

Fig 2: Type of Organization

This area gives data on whether diverse organizations in Afghanistan enlist particular staff for BYOD administration or not. The reason of this result is to get it how organizations consider the preferences and drawbacks of having a committed staff for BYOD issues.

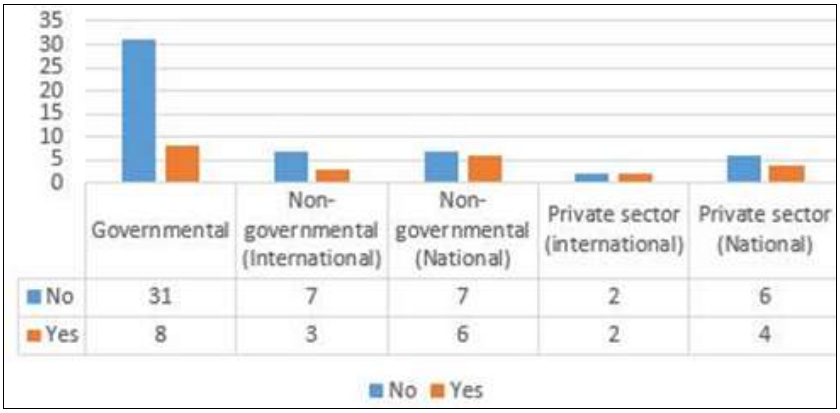

Fig 3: BYOD Management Staff

Figure 3 shows that most of the organizations, particularly, governmental, non-governmental, and private sectors have not hired a dedicated person to look over BYOD management and security issues. In outline, two thirds of the respondents have detailed that their organizations need a particular worker for BYOD. That's to say, two thirds of study members from legislative and non-governmental (worldwide) organizations reported that there's no particular staff for BYOD issues in their organizations. The result assist appears that about half of non-governmental (national) and half of private divisions (worldwide) organizations selected committed staff for BYOD. Most seriously, private divisions (national) by and large don't contract a devoted staff for BYOD. Generally, need of profound understanding on points of interest and impediments of BYOD, lacking information approximately the dangers with BYOD, and budget issues in numerous organizations tend to be the most reasons behind not contracting a committed individual to bargain with BYOD related issues.

C. Awareness and Usage of BYOD

This part of research depicts the level of awareness of IT professionals in different organizations of Afghanistan, and it shows how much BYOD is being used in the workplaces in Afghanistan.

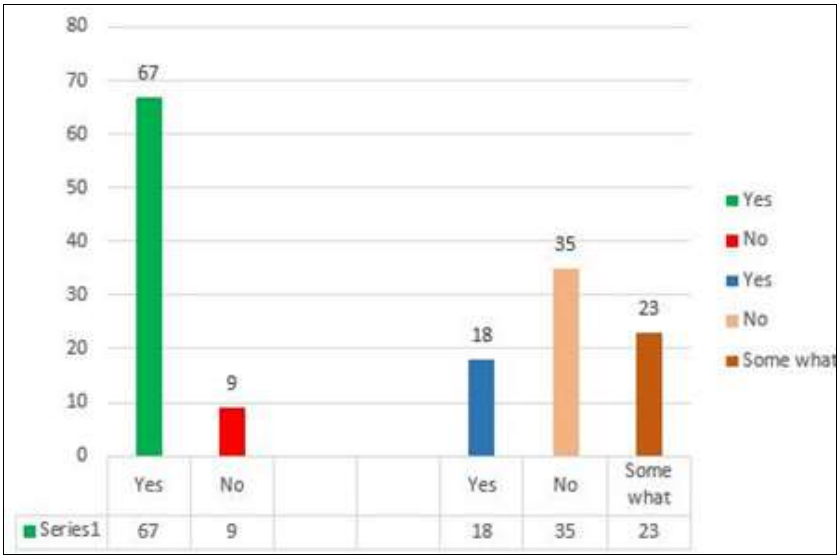

Fig 4: Awareness and Usage of BYOD

The over chart traces the result of mindfulness and utilize of BYOD in several organizations in Afghanistan. Because it can be seen, in spite of gigantic utilize from BYOD, the level of understanding around preferences and dangers of BYOD is impressively moo. In outline, more than three-fourths of the respondents replied that they utilize BYOD gadgets in their organizations; be that as it may the other side of the investigate appears that slightly over three-fourths of the same respondent answered that they either don't get it the concept and dangers of BYOD or they have constrained data approximately it. This finding highlights a concern point related to BYOD utilize in Afghanistan; to put it in an unexpected way, lion's share of the IT experts utilize BYOD without understanding the points of interest and related dangers and dangers of BYOD to their organizations

D. Data Breach Using BYOD in Afghanistan's Organization

This section shows the graph of data breach and leaking using BYOD in different organizations in the country

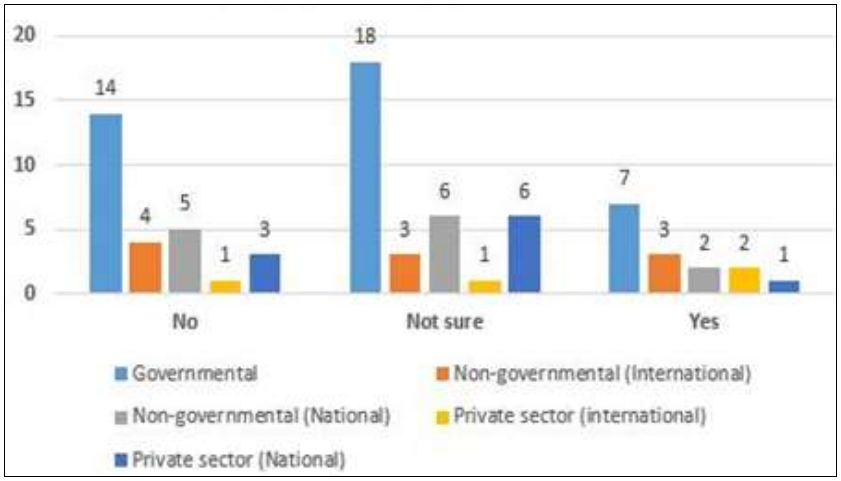

Fig 5: Data Breach Using BYOD in Afghanistan's Organization

The chart within the over uncovers the extent of information breach in numerous organizations in Afghanistan whereas they utilize BYOD. The figure 5 portrays that most of the IT experts who reacted to the study either don't know whether their frameworks are breached whereas they utilize BYOD or they have detailed that their frameworks are misused and data leaking happened. To expand, about half of the respondents have answered that they don't know whether the act of information breach or framework misuses have happened or not, and one-fifths of them replied that the act of information spill and breach has happened in their systems whereas they utilize BYOD; in any case somewhat over one-thirds of the respondents have reacted that they have not confronted any information spill and breach whereas their clients utilize BYOD within the systems. This chart traces that in numerous organizations appropriate framework or controlling machines are not being utilized to distinguish information breach and organize abuse. Moreover, those who answered that they are not beyond any doubt whether system leaking happened or may be since if they don't realize and identify information breach occurrences.

E. Existing BYOD Policy in Organizations

Obviously, not having corporate approaches and measures within the organizations for BYOD is additionally a enormous challenge whereas organizations utilize BYOD. It is critical to standardize and legalize framework utilization utilizing BYOD through arrangements and benchmarks. In this individual, this study has also paid endeavors to look at whether organizations within the nation hold approaches and benchmarks for BYOD or not.

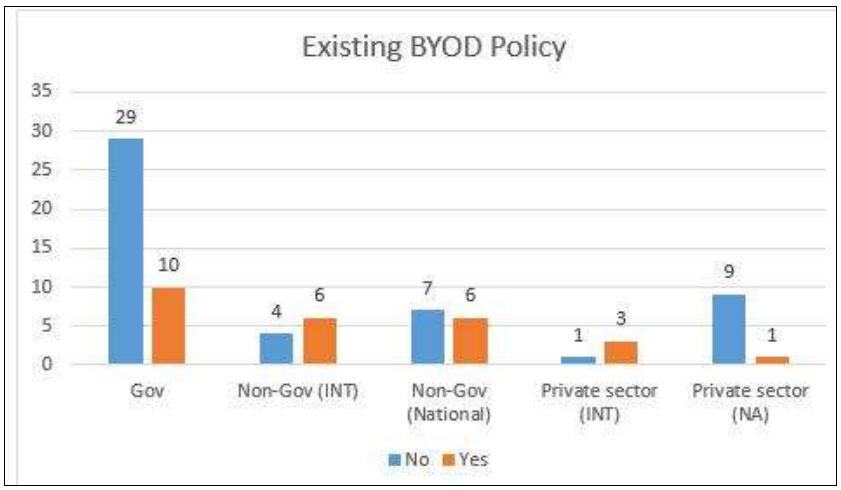

Fig 6: Awareness and usage of BYOD

The figure 6 appears which sorts of organizations consider corporate approach for BYOD, and at the same time it appears how much creating a corporate arrangement for the organizations are been overlooked. As we will see, lion's share of the organizations leans toward to have legitimate systems for BYOD through advancement of arrangements in their organizations. To demonstrate, government organizations with nearly three-fourths of positive reactions have affirmed that they utilize arrangement for BYOD; about half of national and worldwide non-government organization created arrangements for BYOD; over two-thirds of national and worldwide private divisions have answered that they have created arrangements for their organizations. On the other hand, over one-fourth of government organizations, somewhat over half of national and universal non-government organization, and almost one-third of national and universal private segments have reacted that they don't utilize any arrangement for BYOD in their organizations.

F. BYOD Devices Infected by Malware

To identify risks behind BYOD devices in the organizations, this report has also tried to evaluate and understand whether

BYOD devices are infected by malicious applications or not. This section will help the readers to understand how much BYOD devices are susceptible to malwares

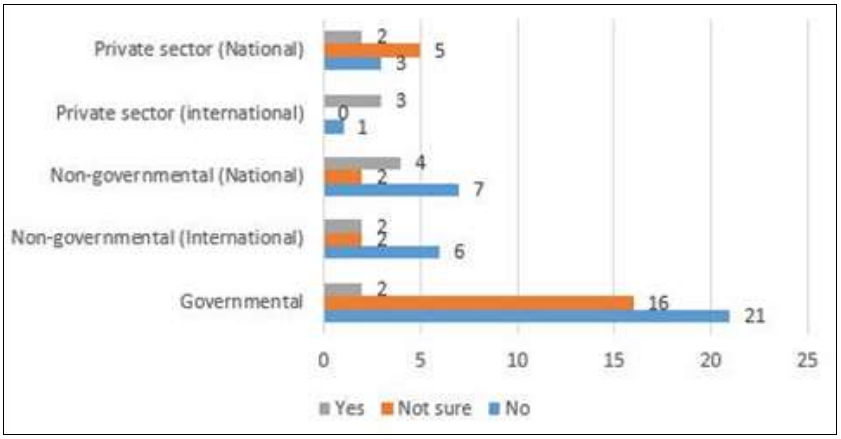

Fig 7: BYOD infected by Malware

The figure 7 uncovers which organization sorts have experienced malwares whereas they utilize BYOD. It is justifiable from the table that numerous organizations have not confronted with malwares in BYOD gadgets. To clarify it assist, over half of government organizations and national/international non-government organizations, and one-third of national and universal private segments are detailed that they have not seen malware contamination within the final 12 months. In any case, underneath half of government and national/international organizations and two-thirds of national and universal private divisions have reacted that they have experienced undesirable applications and malwares with their BYOD gadgets.

G. Usage of Technology in Afghanistan's Organizations

In this section, the purposeful is to reflect information and data around the advances and apparatuses being utilized totally different organizations in regards to oversee and plan cautious measures to the potential dangers and assaults against BYOD gadgets. This will too offer assistance the peruses to know around the advances which organizations utilize, and prescribe for advancement within the regions required.

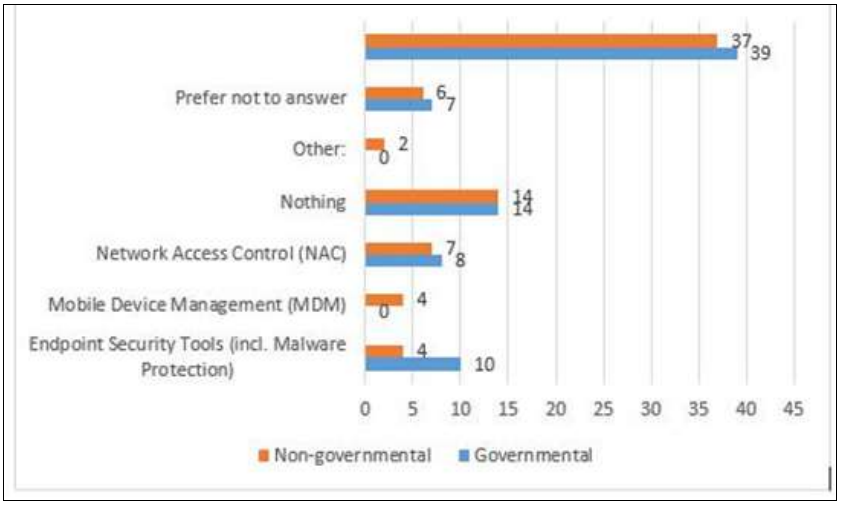

Fig 8: BYOD technology usage

From the figure 14, it is obvious that distinctive organizations utilize distinctive advances and instruments to oversee and secure BYOD gadgets. Concurring to the chart, lion's share of organizations appears utilize a few apparatuses or innovations for BYOD administration and security. In other words, distinctive advances such as NAC, MDM, and endpoint security devices are being utilized in legislative and non-governmental organizations to oversee and screen BYODs in their organizations. As we are able see, a few respondents incline toward not to show the advances and devices they utilize for BYOD management. It is understandable that some organizations and IT professionals refrain to indicate their technologies for security reasons.

H. Technical Staff Concern about BYOD Security

Understanding the concerns and apprehension of IT experts and organizations are imperative. Having profound information approximately the concerns and issues being raised by BYOD clients makes a difference specialists and specialized individuals to plan and move forward innovation to superior react to the dangers and concerns exist against BYOD. Subsequently, this area has assembled figures on how much individuals feel themselves apprehensive almost BYOD and which zones are the greatest concerns.

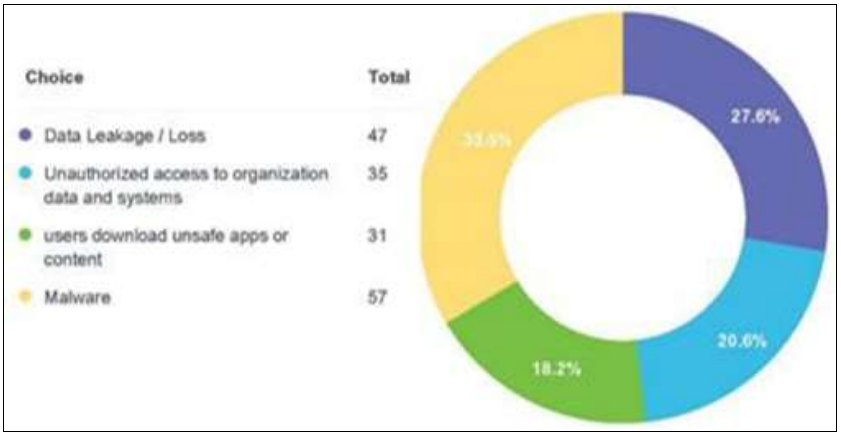

Fig 1: Concerns about BYOD Security

The figure 9 delineates the four major concerning regions related to BYOD. In light of the over chart, malware and information spillage or misplaced of information are the greatest concern of IT experts in connection to BYOD. In clarification, one-thirds of IT experts are concern of malware applications, over one-fourths of experts are stressed of information spillage and burglary of data, somewhat over one-fifths of IT experts are on edge of unauthorized get to to the framework, and underneath one-fifths of them are stressed of downloading hazardous and unreliable applications by conclusion client whereas they actualize BYOD in their organization.

6. Recommendations

The recommendations are suggested in the following table 1

Table 1: Recommendations

S/no	Objectives	Findings	Recommendations
1	To understand the level of awareness of IT personnel about BYOD in Afghanistan	The level of awareness of IT personnel in Afghanistan about BYOD technology is very low.	Ministry of Information and Communication Technology (MoICT) must take initiative to develop a holistic and country wise strategy and policy for increasing and enhancing the awareness of IT personnel in different organizations about BYOD.
		Most of IT personnel working in different organizations do not know whether a data breach using BYOD happened in their organizations or not.	MoICT should provide regular trainings on BYOD, possible threats and data breach to all governmental and non-governmental Organizations' personnel.
2	To evaluate the handling of Cyber threats associated with BYOD	Very few organizations in Afghanistan are using specific technologies for BYOD to handle cyber threats.	Every organization should nominate one focal point for BYOD trainings and these focal points should act as specific responsible body in their organizations in order to combat against data theft, data breach and disseminate information regarding different security issues.
3	To define a secure mechanism for BYOD being used in different organizations to mitigate the risk of BYOD	Unfortunately, very few IT personnel think positively about BYOD. However, majority of them have largely expressed their concerns about BYOD implementations.	Implement the required technologies for security of BYOD such as MDM, MAM, IAM, MAS, DLP, and IDS. Should use the proven reference models for BYOD like MSRA reference model. Every organization must implement BYOD in order to reduce cost and increase productivity due to off-site working from anywhere at any time.

7. Conclusion

The reason of this think about was to get it the issues related to the usage of BYOD within the setting of the Afghanistan's organizations. In this ponder, the creators utilized cross-sectional strategies of collecting and analyzing quantitative information, counting surveys with open and closed-ended questions. The creators discover that the usage of BYOD will bring numerous benefits to the organization. However, after executing BYOD within the organizations, there are numerous dangers and challenges. Luckily, the dangers and challenges related with BYOD talked about in this article can be overcome, and particular moderation solutions and strategies for it have been examined within the inquire about. In expansion, we found that IT staff have a moo level of mindfulness of the dangers and challenges of BYOD security and the most recent innovations utilized by Afghan organizations. At last, this article summarizes the suitable suggestions talked about in Table1.

8. References

1. Young GO. "Synthetic structure of industrial plastics (Book style with paper title and editor)," in *Plastics*, 2nd ed. J Peters, Ed. New York: McGraw-Hill, 1964;3:15-64.

2. Chen WK. Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, 123-135.
3. Poor H. An Introduction to Signal Detection and Estimation. New York: Springer-Verlag, 1985, Ch. 4.
4. Smith B. "An approach to graphs of linear forms (Unpublished work style)," unpublished.
5. Miller EH. "A note on reflector arrays (Periodical style—Accepted for publication)," IEEE Trans. Antennas Propagat to be published.
6. Wang J. "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," IEEE J. Quantum Electron submitted for publication.
7. Kaufman CJ. Rocky Mountain Research Lab., Boulder, CO, private communication. 1995 May.
8. Yorozu Y, Hirano M, Oka K, Tagawa Y. "Electron spectroscopy studies on magneto-optical media and plastic substrate interfaces (Translation Journals style)," IEEE Transl. J Magn. JPN. 1987 Aug;2:740–741. [Dig. 9th Annu. Conf. Magnetics Japan, 1982, p. 301].
9. Young M. The Techincal Writers Handbook. Mill Valley, CA: University Science, 1989. (Basic Book/Monograph Online Sources) J. K. Author. (year, month, day). Title (edition) [Type of medium]. Volume (issue). Available: http://www.(URL)
10. Jones J. (1991, May 10). Networks (2nd ed.) [Online]. Available: http://www.atm.com
11. (Journal Online Sources style) K. Author. (year, month). Title. *Journal* [Type of medium] (issue), paging if given. Available: http://www.(URL) research work, membership, achievements, with_photo that will be maximum 200-400 words