Journal of Information Systems & Information Technology (JISIT) *Vol. 3 No. 2 2018*
ISSN: 2478-0677

Bring Your Own Device (BYOD) – "Angel or Demon": A Conceptual Review

Razik Kariapper Ahmadh Rifai Kariapper [1], Mohamed Satheek Suhail Razeeth [2]

[1] Faculty of Technology,
South Eastern University of Sri Lanka,

[2] Faculty of Applied Sciences,
Sabaragamuwa University of Sri Lanka,
rk@seu.ac.lk, razeethsuhail@gmail.com

Abstract. Bring your own device (BYOD) is a way to connect employee devices to the organization's network for routine tasks. The idea was developed for many purposes in the early 20th century. It offers incentives to workers and organizations in various fields. However, this concept delivers its upsides and downsides in various field. The benefits and drawbacks vary by domain area. This study aims to analyze past studies' literature to recognize the ups and downs of various domains. a systemic literature review approach has been taken to perform the review. Besides, a proper and standard guideline was adopted and proposed for this systematic analysis. This study also aims to develop a conceptual solution. The sensitive data of the organization is not secure when an employee deals with BYOD. When they work with their own devices, an organization's data is stored in their devices, so a higher chance of the possibility of leakage or loss. The only emerging and sophisticated approach to solving this problem is cloud computing, along with cellphone jammer and autocratic leadership, which is a triple constraints concept, proposed for effectively utilizing the BYOD. The same concept can be extended to primary and secondary schools; and event to conduct the exams also.

Keywords: BYOD, Triple constraint concept, Cloud Computing, Cellphone jammer, Autocratic leadership

1 Introduction

In today's competitive environment, people's working and personal life interrelated. There are many possibilities of handing private life during the work environment and vice-versa. With the rapidly evolving technical factor and rising workload, the deadline has many problems. Even after working hours, an employee must work to meet the deadline. It has complicated the employee's private and personal life, contributing to an unsatisfactory life. Most workers, however, prefer to work after office hours in their comfortable atmosphere rather than the working environment. The organization's conventional operating method offers this principle less flexibility, so workers work with a grievance.

Bringing your own device(BYOD) is a way to connect employee devices to the organization's network for routine tasks [1]–[6]. By comparison, the company allowed workers to carry their own gadgets to work-related practices. This idea was developed for many purposes in the early 20th century. It offers incentives to workers and organizations in various fields. Many domains have recently been adapted for many purposes. BYOD

recognizes offices, the medical domain [7]–[9], higher education [10], [11], and healthcare sectors as core fields.

Without any benefits, nobody ever adapts technology or principle. In that respect, this idea delivers a robust and better solution for both users and administrators. The advantages are known as; decreases procurement costs, increases workplace flexibility, job satisfaction, empowered working condition, enhances efficiency and reduces work hours. Besides these few benefits, users and administrators have far more. However, the drawbacks are described as; Non-work-related activities, the risk of losing core competencies, privacy concerns, and rapidly evolving technologies. Likewise, this concept delivers its upsides and downsides in various fields. The benefits and drawbacks vary by domain area.

Whenever we adopt new technologies or concepts, it always had its angel and demon sides. When we follow a proper and set of pre-defined guidelines based on the issues, technology becomes the best suite. This study aims to analyze past studies' literature to recognize the ups and downs of various domains. This study also aims to provide a conceptual approach and collection of guidelines to make this idea appropriate in different fields.

2 Literature Survey

[12] Found a concept of BYOD in a business context. From the study, they found that a company earns an additional 1.7 million USD with 1,000 own devices of the staffs. Also, they found that when a user works with their own devices reduces unnecessary issues in a working environment. A new operating system, hardware issues, network traffic, and learning new technologies are the most identified issues and which is reduced considerably while using the concept of BYOD.

As mentioned by [13], It could be noted that BYOD and cloud computing seem to be the two factors that provide and control information technology security these days.

[14] Stated that applying BYOD in the working sector enhances employees' flexibility, versatility, efficiency, and engagement. These are the primary reasons why BYOD is prevalent across various industries. Meanwhile, they also detailed that allowing the BYOD concept sometimes leads the wrong path and which affect the work-related activities mostly. When working with BYOD, an employee can access non-work-related activities like spending time on social networking rather than doing assigned work. Hence this concept is not applicable for every place except for some.

[15] Studied the threads and security issues of BYOD. The study defined and grouped into two types, namely tangible and intangible threads. Tangible threads deal with the loss or heist of the devices. At the same time, intangibles explain digital security issues like virus and malware attacks. Parallelly, [16] stated that the data generated from smart devices are pervasive. It contains the essential privacy information of the user. Whenever it losses or get cyber-attacks, the consequence cannot be imaginable.

[17] Explored the legal issues of implementing BYOD. From the analysis, we were able to identify that BYOD has a greater risk and harmful consequences on the company even though it has some benefits.

Whenever an employer using their own devices, organization and users getting benefits differently. The needless expense of purchasing equipment for the company is minimized. Simultaneously, the user feels relaxed and happy by using their own devices [18]. Also, indicated said that BYOD improves the versatility, accessibility, and portability of devices to appeal to their employees' process.

[19], from a reliable web source, found that 60 percent of the company enables workers to use BYOD. 26% are not permitted by now; around 14% of the company has no idea to allow employees to use BYOD.

[20] Stated that when an organization allows BYOD, there is a possibility of doing other work rather than task due to the different attraction from allowed devices. Therefore they suggested that there must be a proper procedure and architecture for monitor users.

[21] Very clearly debated that when a user keeps the organization's data in personal devices, there are higher possibilities of losing those data. This process leads to massive complexity among organizations in a different way. Also, smart devices' storage devices may enclose the organization's data to the public very quickly. Therefore, it is complicated to maintain data integrity when using BYOD among business and small-medium organizations.

[22] Suggested that BYOD is one of the best ways to identify an excellent employee for an enterprise. Also, [23] mentioned that the BYOD concept connected employees with their own devices. Therefore, there is no need for internet connectivity for sharing and communicating with each other—this reduced the unnecessary cost of an organization considerably.

[24] specified that whenever employees using their own devices within the organization provides optimum quality and more independence in case of the decision-making process. Besides, [25] stated that it increases the creativity of an employee.

Many studies mentioned that using BOYD concept in an organization reduce the unnecessary cost. However, [18] et al. debated that employees are typically obtaining payment for the services of their own devices from the organization. So we cannot be agreed on other previous studies.

Several studies with authors identify the employers' intention to use BYOD among different sectors. Information systems theory was applied to the study. Many authors' results revealed that employees use this concept due to ease of use [23], [26]–[31]. Simultaneously, some other studies found that employees perceive usefulness whenever they use their device to work [26], [32]–[34].

[35] et al. accomplished a study with BYOD in science education for primary students. In this study, students are allowed to use their own devices with familiar apps. The study was conducted with pre-test and post-test. At the end of the study, student knowledge was increased in a science subject, and BYOD positively impacts the learning activities of students.

[36] Revealed that nowadays, Youngers even have perfect knowledge in technological sites. They prefer to work with familiar devices; hence, the BYOD concept provides an excellent platform to digital age young workers.

As specified by [37] that not only smart devices but also any devices that are preferred by users are identified as BYOD devices.

As a result, obtained from [38], it could be enclosed that 71% of global companies permitted their employers to work with the BYOD concept. Another similar measurement from [39] shows that from 2012 to 2013, many countries changed their work-related tricks with BYOD. Plenty of the changes in the US, Asia, and the US were 18 percent, 77 percent, and 43 percent, respectively.

[40] et al. have examined the idea of BYOD between medical schools and healthcare institutions. This analysis established a review matrix to classify an article that meets the purpose of the study. From the matrix, 14 papers were generated that correspond precisely to the criteria. As a result, guidelines for "Device Management, Data Security, Medical Applications, Information Technology, Education and Curriculum Policy" have been developed for schools and healthcare use by BYOD.

The use of the BYOD framework has provided major pros to medical students' pedagogical activities. The medical institution and the healthcare system do not need to purchase the appliances. Instead, students use their own equipment for learning activities; thus, the cost of the schools and the institute is substantially reduced by BYOD [41]–[44]. Also, students and employees effective and working with creativity with BYOD when compared with the traditional way [45]–[48]. Furthermore, this concept increases the output and job gratification of an employee. The BYOD enables medical students and employers to exchange data in the desired format [49] with easy access [50]–[52]. Mostly, students do not need an internet connection to transfer content when working with their own device [53].

Many studies mentioned that in the medical sector, without having proper instruction leads BYOD in a challenging way. Also, many studies stated that policies of how to use BYOD needs to implement to have a better working environment [44], [54]–[56]. When students and employees have no restrictions, several problems arise in the working and learning environment. The identified issues are security issues and unsuitable utilization of devices [44], [57]–[62]. These issues lead to attracting students and employees from doing their work to other sides. Which directly affects the educations and communication of students and employees [63], [64].

Many studies have differently explored the student's examination with BYOD [65]–[68]. [69] Discussed e-assessment with BYOD. This study sorted out essential and exciting aspects. Whenever students using their own devices, there is no need for a separate room to doing that, and students can be done in their independent environment. Also, this study provided solutions for examinations are "bootable USB Stick with a Linux system" and "virtual desktop infrastructure". Typically, the examination process needs more resources, including the classroom, human resources, and specific time. However, working with BYOD eliminates unnecessary needs. On the other hand, introducing BYOD in assignments and examinations will carry different issues. Encounter those issues, specific applications, or software needs to install in the students' own devices before they start.

There are several criticism and debates among individuals and professionals about adapting BYOD among schools and secondary educations. [70] & [71] stated that in the current digital era, students must adapt to technological solutions to bright their future in technological sides. Also, they need to adapt to changes in society. As a support to that argument, [72] mentioned that digital learning must be mixed with the traditional learning method for improving pedagogical activities. When the traditional method integrates with the BYOD concept, the students' curriculum also gets stronger parallelly [73]. Nevertheless, there is another statement from other studies that with financial barriers, every parent and school cannot have a proper BYOD device for studies. However, [74] stated a solution to supporting funding from different tactics to have a BYOD concept in schools.

[75] Indicated that the BYOD improved the result of the students considerably. Concurrently, Sharples [76] directed that BYOD delivers a different attraction to students than an improving learning outcome. As a support to Sharples, [77] mentioned that the student's insufficient knowledge regarding the BYOD increases "cyber-bullying" [78]–[81].

[82] et al. identified the management issues of BYOD as a survey. Through this study, they have proposed a framework for overcoming most security problems of BYOD. The proposed framework contains three phases, namely, analysis, design, and action. At the end of the study, they pointed out twelve issues and which will address in the next study.

The BOYD concept saves a lot of useful resources. In that regard, as stated by [83], it could see that the BYOD user saves an average of 47 minutes per day. This amount increased to 2 million hours per year. Also, [84] reported that BYOD improves the flexibility of employers as their desire. This idea of BYOD helps and stimulates to work from home concept without any complexity. However, [85] stated that BYOD creates

unnecessary stress regarding family even when in the working environment, which distracts the employee from work.

[86] Reported a significant point regarding security and BYOD. Employers and users using a variety of software and application on their own devices and which uses several networks. The network they are using may be insecure and unsafe, so there are higher possibilities of losing the company's sensitive data. When the employee stores sensitive data to their own preferred devices, proper security protocols are necessary. When the user gives authenticity, then data become whom property? In this situation, data protection is impossible [87].

3 Methodology

This study focuses specifically on a review study; thus, a systemic literature review approach has been taken to perform the review. Besides, a proper and standard guideline was adopted and proposed for this systematic analysis. The following research concerns and objectives were categorized for analysis

Table 1. Research Problems and motivations

Research Problem	Aim / Objectives
Domains	Identifying all BYOD domains in the current era
Challenges	Recognize all challenges to deliver a proper solution
Opportunities	Recognize the opportunities to increase the effectiveness and efficiency of the concept.
Advantages	Identify the advantages of having BYOD and apply it to a new domain for solving many issues
Disadvantage	Find the disadvantage for avoiding the use of BYOD from that area

More than 100 papers were searched, selected, and filtered from different digital libraries. Most of the papers were found between 2010 – 2018. The articles are categorized from the peer-reviewed and h-indexed, including Scopus, Science citation index (SCI) journals, conference proceedings, and magazines. The following figure elaborates the way of the selected article for this study.

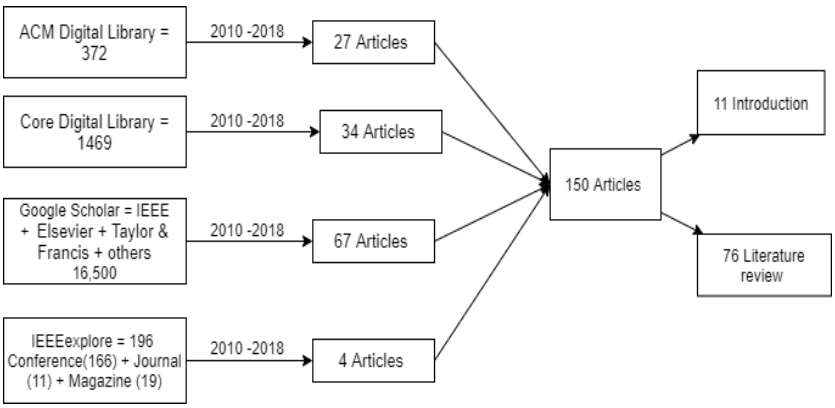

Figure 1: Article selection process

The manual process was carried out to identify the relevant article of this study. Empirical studies, keywords, and abstracts are helped to found the selected articles. This study also aims to develop a conceptual solution based on the identified research problems. The solution will be focused on current trend technological aspects

4 Results and Discussion

Table 2 Different domins with BYOD with issues

BYOD Domain	Challenges / Disadvantages	Opportunities / Advantages
Organization/ Office /company	1. New operating system 2. Number of hardware 3. Network traffic 4. Adopt new technologies 5. Engaging non-work-related activities. Example. Facebook usage 6. Devices can loss 7. Virus and malware problems 8. Privacy issues 9. Possibilities of sensitive data loss	1. Enhances employees' flexibility, versatility, efficiency, and engagement 2. Equipment purchasing cost reduced 3. Employers obtain happiness and satisfaction 4. Improves the versatility, accessibility, and portability of devices 5. Identification of an excellent employee 6. No need for an internet connection always 7. Independent decision-making 8. Improve creativity of employee 9. Reduce the company's unnecessary cost 10. Ease of use and usefulness 11. Provides the best platform to work
Science education for primary students	1. Different attraction than learning	1. Improves the science knowledge of the students
Medical higher education and health institution	1. Device Management and Data Security of medical Applications 2. Cannot apply without proper instructions and guidelines 3. Need a sophisticated working environment 4. Security issues and data leakage 5. Attract students differently and provides restrictions on	1. Institution or college does not buy medical equipment, and student use their own, which reduce cost 2. Sufficient work and learn with creativity 3. Increase productivity, Job Satisfaction, Satisfaction in learning 4. Data transfer happens in the desired format, and the internet

	education and the working process.	not necessary always
Examinations and assessments	1. Needs resources, including the classroom, human resources, and specific time. 2. Challenging to follow examination in a proper way	1. No need for a separate room 2. Independence and freedom to do an assessment
Schools and secondary educations	1. Financial problems of parents and the schools 2. Motives students other than learning 3. Higher possibility of cyber-bulling	1. Improve technical skills of a student 2. Adapt the society with current trends 3. Improve pedagogical activities 4. Enhance curriculum 5. Improves the outcome or result in a specific field
Management	1. Managing security issues	1. Greater flexibility in the handling of work and non-work-related activities.
An employee of any domains	1. Family stress distracts the work.	1. Save a certain amount of working time per day 2. Flexible working environment 3. Promote work from home concept with satisfaction
Security	1. insecure and unsafe 2. Possibility of losing sensitive data	1. User learn new technologies regarding security

Table 2 above clearly illustrates the various domains of the BYOD based on the selected papers and the threats and implications. Looking deeply at the table, we could identify that the BYOD idea seems to have its benefits and drawbacks. It also ensures that there are equal opportunities for problems and the treatment of BYOD in various domains. However, allowing the drawback of the concept is not the right approach. We need to seek solutions for converts challenges into possibilities. Also, we need to reduce the challenges as minimum as possible. Therefore this study further considers the conceptual approach with the technical solution.

4.1 Proposed Model

This study focused on the conceptual framework for different domains with the technical component

4.1.1 Organization / Company / Office model and components

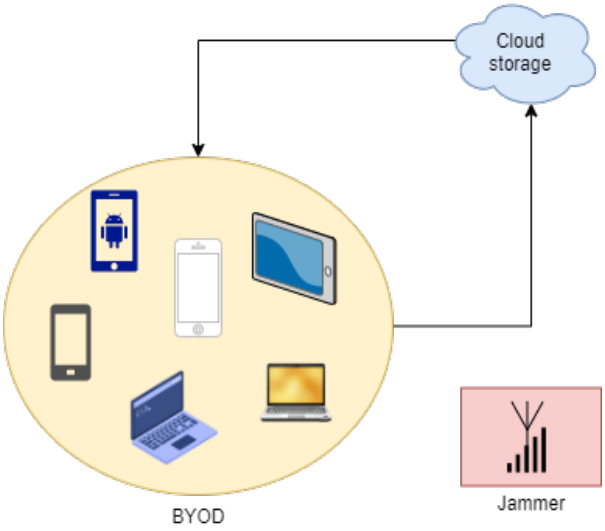

Figure 2: BYOD with cloud

Figure 2 shows the conceptual structure of any organization which is dealing with sensitive information. Typically, several studies mentioned and directed that the sensitive data of the organization is not secure when an employee deals with BYOD. When they work with their own devices, an organization's data is stored in their devices, so a higher chance of the possibility of leakage or loss. This is one of the fundamental and unsolvable mystery up to now. It is another significant reason why the organization is not allowing the BYOD concept inside the organization even when it provides advantages. The only emerging and sophisticated approach to solving this problem is cloud computing. When a user using the cloud concept, they do not need to store the sensitive data into their device. Instead, they can work with the organization data stored in the cloud by log in user authentication. If the user wants to work with BYOD, then they need to access the data with the organization's cloud account. However, the employers lose their devices, no need to fear about the organization's data. Without knowing the authenticity, it is not possible to access all data.

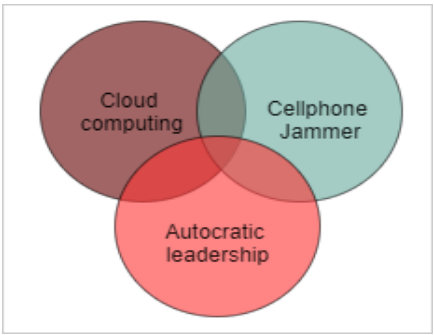

Figure 3: Conceptual triple constraints of BYOD in an organization

On the other hand, there are many possibilities for using non-work-related content when employers utilize BYOD. The possible approach to this issue is blocking the unnecessary applications of their own devices. It means employers are only allowed to use the company network, whether it is wired or wireless. They cannot use their own device for internet connectivity. In this context, there must be followed by an autocratic leadership style. When the employers using the organization's network, unnecessary applications and webpages will be blocked with Internet protocols. Albeit, as a human there are higher possibilities to connect with another network to do other activities. A normal human being would not like to do their job continually. The jammers play a crucial role here in avoiding this issue. When an organization uses a cell phone jammer, the employee must adapt their organization's network even without their wish. Furthermore, if the user tries to go with a VPN, they want to block that by autocratic leadership style. These triple constraints change the use of BYOD from demons to angle among the organization.

4.1.2 Primary and Secondary school model

The student model does not need any cloud concept or a jammer concept. Specific applications or web pages created by an authority are required to carry out this model. In this model, we can propose some guidelines to make the BYOD an angel. Following conceptual guidelines shows how a primary and secondary school need to adapt to the BYOD,

1. Schools need to create their own networks to connect student's own devices.
2. Students must use approved apps or web pages during pedagogical activities.
3. Other applications and webpages must be blocked using IP (Specifically social media)
4. Students need to monitor by parents, and teachers continue to avoid cyber-bullying issues. Also, proper knowledge must be provided to the students regarding the cyber-bullying concept.
5. If possible, the school needs to develop or buy specific pedagogy applications or websites like K-12 for the learning process.
6. When allowing the BYOD to the school, each parent does not have financial strength. Therefore, need to implement the funding concept mentioned by Bailey, Schneider & Vander Ark.
7. When students use the BYOD concept, they should use their devices with flight mode. It will not disturb learning and teaching activities.
8. Generally, when teachers utilize BYOD, there is a possibility of not following guidelines. Here, there must be an autocratic leadership style must be followed by principles.

Here we have given eighth conceptual guidelines for avoiding the BYOD concept's challenges among primary and secondary schools.

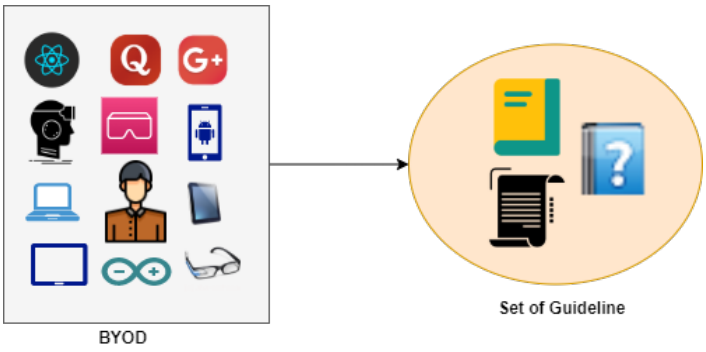

Figure 4: BYOD and set of instruction for schools

4.1.3 Examination model and ways using BYOD

The examinations are a callous mechanism with the BYOD approach. There are many possibilities of violations and cheating when we are dealing with the BYOD concept. Though it reduces unnecessary human and cost, it is useless if any cheating happens. Therefore this study seeks a better way to tackle this issue. There are several ideas we can follow to sort out these issues. Following shows some approaches to deal with the examination with BYOD

1. Change the examination modes

The final examination can be changed as an oral test or viva to utilize the BYOD in examination domains. If we deal with oral or viva video conference using their own devices in any places possible. This mode of examination will reduce unnecessary costs and space. Also, students getting the same knowledge as they are writing in the final exams.

2. Total control of the device by supervisors

It is another approach that we can deal with the BYOD in the examination. In this idea, the person who conducts the examination has controlled the BYOD devices with some mechanism. When the devices control by another person, there are very minimal chances to do a cheating activity.

3. A virtual machine in the BYOD device

A virtual machine is placed in a specific place by an examination organization. The virtual machine and its operating system should access by the BYOD device. All examination questions have been prepared in that OS. Once the student login into the system, they can continue their exam as tradition. Here additional surveillance must be placed for monitoring student's activity. Therefore, students must turn on their cameras to do their examination.

5 Conclusion

Many scholars have conducted many studies in various BYOD domains. In numerous areas, this is a highly suitable and meaningful method for getting the best output. Throughout the analysis, we could determine that this idea has its angel and demon faces. The benefits and drawbacks of this concept are equal opportunities. When we obey proper guidelines and rules in a particular domain, this concept's performance is exceptionally significant. Many countries have already adapted and ask their workers to change this to minimize the undue burden. Users like and embrace this concept due to its simplicity and comfort. It has several pitfalls in the complex domain. When Improving and exploring remedies to this limitation will help overcome some complications robustly.

References

[1] P. Hynes and S. Younie, "Bring your own device?," in *Debates in Computing and ICT Education*, 2018.

[2] L. Bennett and H. Tucker, "Bring Your Own Device," *ITNOW*, 2012, doi: 10.1093/itnow/bws010.

[3] C. Van Wingerden, A. Lidz, A. Barse, J. DeMark, and D. Hamiter, "Bring Your Own Device (BYOD)," in *Information and Technology Literacy*, 2017.

[4] S. Miller and K. E. Welsh, “Bring Your Own Device (BYOD) in higher education: Opportunities and challenges,” in *Mobile Learning: Students’ Perspectives, Applications and Challenges*, 2017.
[5] B. Hayes and K. Kotwica, *Bring Your Own Device (BYOD) to Work*. 2013.
[6] G. Disterer and C. Kleiner, “BYOD Bring Your Own Device,” *Procedia Technol.*, 2013, doi: 10.1016/j.protcy.2013.12.005.
[7] J. Keyes, *BYOD for Healthcare*. 2014.
[8] F. Portela, A. Moreira da Veiga, and M. F. Santos, “Benefits of Bring Your Own Device in Healthcare,” 2017.
[9] P. Y. Moore, “Factors Influencing the Adoption of Bring Your Own Device Policies in the United States Healthcare Industry,” *ProQuest Diss. Theses*, 2018.
[10] S. Difilipo, “The policy of BYOD: Considerations for higher education,” *EducauseReview*, 2013.
[11] K. Sangani, “BYOD to the classroom [bring your own device],” *Eng. Technol.*, 2013, doi: 10.1049/et.2013.0304.
[12] C. Rose, “BYOD: An Examination Of Bring Your Own Device In Business,” *Rev. Bus. Inf. Syst.*, vol. 17, no. 2, pp. 65–70, 2013, doi: 10.19030/rbis.v17i2.7846.
[13] Gartner, “Gartner IT Glossary,” 2012. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/consumerization. [Accessed: 20-Jan-2018].
[14] K. Dery and J. MacCormick, “Managing mobile technology: The shift from mobility to connectivity,” *MIS Q. Exec.*, 2012.
[15] B. Markelj and I. Bernik, “Mobile devices and corporate data security,” *Int. J. Educ. Inf. Technol.*, 2012.
[16] S. Mahesh and A. Hooter, “Managing and Securing Business Networks in the Smartphone Era,” *Fifth Annu. Gen. Bus. Conf. Sam Houst. State Univ. Huntsville, Texas*, 2013.
[17] M. Dhingra, “Legal Issues in Secure Implementation of Bring Your Own Device (BYOD),” *Phys. Procedia*, vol. 78, no. December 2015, pp. 179–184, 2016, doi: 10.1016/j.procs.2016.02.030.
[18] A. M. French, C. J. Guo, and J. P. Shim, “Current status, issues, and future of bring your own device (BYOD),” *Commun. Assoc. Inf. Syst.*, 2014, doi: 10.17705/1cais.03510.
[19] T. Hammond, “Current BYOD usage,” 2015. [Online]. Available: https://www.zdnet.com/article/ces-2015-d-link-breaks-1gbps-wi-fi-speed-barrier/. [Accessed: 02-Jan-2018].
[20] P. Pavón and Risky, “Business: ‘Bring-Your-Own-Device’ and Your Company.” [Online]. Available: https://www.americanbar.org/groups/business_law/publications/. [Accessed: 05-Jan-2018].
[21] J. Robert and Mavretich, “Legal Issues within Corporate ‘Bring Your Own Device’ Programs,” *Sans Institute, May*, 2012.
[22] M. Loose, A. Weeger, and H. Gewald, “Byod - The next big thing in recruiting? examining the determinants of BYOD service adoption behavior from the perspective of future employees,” in *19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime*, 2013.
[23] N. Zahadat, P. Blessner, T. Blackburn, and B. A. Olson, “BYOD security engineering: A framework and its analysis,” *Comput. Secur.*, 2015, doi: 10.1016/j.cose.2015.06.011.
[24] A. Weeger and G. Heiko, “Factors influencing future employees’ decision-making to participate in a byod program: Does risk matter?,” in *ECIS 2014 Proceedings - 22nd European Conference on Information Systems*, 2014.
[25] A. Leclercq-Vandelannoitte, “Leaving employees to their own devices: new practices in the workplace,” *J. Bus. Strategy*, 2015, doi: 10.1108/JBS-08-2014-0100.
[26] R. Buettner, “Towards a new personal information technology acceptance model: Conceptualization and empirical evidence from a bring your own device dataset,” in

2015 Americas Conference on Information Systems, AMCIS 2015, 2015.

[27] H. Nathan, S. Allan, and T. Mary, "Motivations for BYOD: An investigation of the contents of a 21st century school bag," in *ECIS 2013 - Proceedings of the 21st European Conference on Information Systems*, 2013.

[28] B. Niehaves, S. Köffer, and K. Ortbach, "IT consumerization - A theory and practice review," in *18th Americas Conference on Information Systems 2012, AMCIS 2012*, 2012.

[29] K. Ortbach, "Unraveling the effect of personal innovativeness on bring-your-own-device(byod) intention - the role of perceptions towards enterprise-provided and privatelyowned technologies," in *23rd European Conference on Information Systems, ECIS 2015*, 2015.

[30] K. Ortbach, N. Walter, and A. Öksüz, "Are You Ready To Lose Control ? A Theory on the Role of Trust and Risk Perception on Bring-Your-Own-Device Policy and Information System Service Quality," in *ECIS 2015 Research-in-Progress Papers*, 2015.

[31] D. Rivera, G. George, P. Peter, S. Muralidharan, and S. Khanum, "Analysis of security controls for BYOD (bring your own device)," 2013.

[32] C. W. Chen, "BYOD flexibility: The effects of flexibility of multiple IT device use on users' attitudes and continuance intention: Research-in-progress," in *20th Americas Conference on Information Systems, AMCIS 2014*, 2014.

[33] B. Lebek, K. Degirmenci, and M. H. Breitner, "Investigating the influence of security, privacy, and legal concerns on employees' intention to use byod mobile devices," in *19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime*, 2013.

[34] J. Lee, R. E. Crossler, and M. Warkentin, "Implications of monitoring mechanisms on Bring Your Own Device (BYOD) adoption," in *International Conference on Information Systems (ICIS 2013): Reshaping Society Through Information Systems Design*, 2013.

[35] Y. Song *et al.*, "Author ' s personal copy Computers & Education ' Bring Your Own Device (BYOD) ' for seamless science inquiry in a primary school," *El Sevier*, vol. 74, no. 1, p. 12, 2014.

[36] S. Mansfield-Devine, "Interview: BYOD and the enterprise network," *Comput. Fraud Secur.*, vol. 2012, no. 4, pp. 14–17, 2012.

[37] G. Thomson, "BYOD: Enabling the chaos," *Netw. Secur.*, 2012, doi: 10.1016/S1353-4858(12)70013-2.

[38] L. Y. Qing, "BYOD on rise in Asia, but challenges remain," *ZDNet.*, 2013. [Online]. Available: https://www.zdnet.com/article/byod-on-rise-in-asia-but-challenges-remain/. [Accessed: 29-Jul-2013].

[39] A. Nusca, "BYOD: North America and Asia embrace it; Western Europe, not so much," 2013. [Online]. Available: https://www.zdnet.com/article/byod-north-america-and-asia-embrace-it-western-europe-not-so-much/. [Accessed: 29-Jul-2013].

[40] K. Kadimo *et al.*, "Bring-your-own-device in medical schools and healthcare facilities: A review of the literature," *Int. J. Med. Inform.*, vol. 119, no. July, pp. 94–102, 2018, doi: 10.1016/j.ijmedinf.2018.09.013.

[41] S. Nisar and W. R. bt S. Osman, "ICT Transformation through Byod Adoption in Healthcare of Pakistan," *Int. J. Comput. Sci. Commun. Networks*, 2017.

[42] H. Ansaldi, "Addressing the Challenges of the 'Bring Your Own Device' Opportunity.," *CPA J.*, 2013.

[43] M. Olalere, M. T. Abdullah, R. Mahmod, and A. Abdullah, "A Review of Bring Your Own Device on Security Issues," *SAGE Open*, 2015, doi: 10.1177/2158244015580372.

[44] S. U. Al Ayubi, A. Pelletier, G. Sunthara, N. Gujral, V. Mittal, and F. C. Bourgeois, "A mobile app development guideline for hospital settings: Maximizing the use of and minimizing the security risks of 'bring your own devices' policies," *JMIR mHealth uHealth*, 2016, doi: 10.2196/mhealth.4424.

[45] S. Köffer, K. C. Ortbach, and B. Niehaves, "Exploring the relationship between IT

consumerization and job performance: A theoretical framework for future research," *Commun. Assoc. Inf. Syst.*, 2014, doi: 10.17705/1cais.03514.

[46] S. Köffer, K. Ortbach, I. Junglas, B. Niehaves, and J. Harris, "Innovation Through BYOD? The Influence of IT Consumerization on Individual IT Innovation Behavior," *Bus. Inf. Syst. Eng.*, 2015, doi: 10.1007/s12599-015-0387-z.

[47] D. Moschella, D. Neal, P. Opperman, and J. Taylor, "The 'Consumerization' of Information Technology Position Paper," *Csc*, 2004.

[48] F. Gens, D. Levitas, and R. Sega, "2011 Consumerization of IT Study : Closing the ' Consumerization Gap ,'" *Idc*, 2011.

[49] D. Nestel *et al.*, "Evaluation of mobile learning: Students' experiences in a new rural-based medical school," *BMC Med. Educ.*, 2010, doi: 10.1186/1472-6920-10-57.

[50] J. E. Moyer, "Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage," *Journal of Hospital Librarianship*. 2013, doi: 10.1080/15323269.2013.798768.

[51] J. T. Boruff and D. Storie, "Mobile devices in medicine: A survey of how medical students, residents, and faculty use smartphones and other mobile devices to find information," *J. Med. Libr. Assoc.*, 2014, doi: 10.3163/1536-5050.102.1.006.

[52] A. Baheerathan and H. Selvaskandan, "Smartphones and medical education," *Clin. Teach.*, 2014, doi: 10.1111/tct.12169.

[53] W. Hardyman, A. Bullock, A. Brown, S. Carter-Ingram, and M. Stacey, "Mobile technology supporting trainee doctors' workplace learning and patient care: An evaluation," *BMC Med. Educ.*, 2013, doi: 10.1186/1472-6920-13-6.

[54] M. C. Faulds *et al.*, "The feasibility of using 'bring your own device' (BYOD) technology for electronic data capture in multicentre medical audit and research," *Anaesthesia*, 2016, doi: 10.1111/anae.13268.

[55] K. AlHarthy and W. Shawkat, "Implement network security control solutions in BYOD environment," in *Proceedings - 2013 IEEE International Conference on Control System, Computing and Engineering, ICCSCE 2013*, 2013, doi: 10.1109/ICCSCE.2013.6719923.

[56] E. C. Whipple, K. L. Allgood, and E. M. Larue, "Third-year medical students' knowledge of privacy and security issues concerning mobile devices," *Med. Teach.*, 2012, doi: 10.3109/0142159X.2012.670319.

[57] J. Williams, "Left to their own devices: How healthcare organizations are tackling the BYOD trend," *Biomed. Instrum. Technol.*, 2014, doi: 10.2345/0899-8205-48.5.327.

[58] K. Tran, D. Morra, V. Lo, S. D. Quan, H. Abrams, and R. C. Wu, "Medical students and personal smartphones in the clinical environment: The impact on confidentiality of personal health information and professionalism," *J. Med. Internet Res.*, 2014, doi: 10.2196/jmir.3138.

[59] J. Goldfarb, A. Kayssi, K. Devon, P. G. Rossos, and T. D. Cil, "Smartphones and patient care: exploring the use of text-based messaging for patient-related communication," *Surg. Innov.*, vol. 23, no. 3, pp. 305–308, 2016.

[60] A. C. Johnson, S. C. El Hajj, J. N. Perret, T. S. Caffery, G. N. Jones, and M. W. Musso, "Smartphones in Medicine: Emerging Practices in an Academic Medical Center," *J. Med. Syst.*, 2015, doi: 10.1007/s10916-014-0164-4.

[61] P. O'Connor *et al.*, "Interns and their smartphones: Use for clinical practice," *Postgrad. Med. J.*, 2014, doi: 10.1136/postgradmedj-2013-131930.

[62] T. Ealey, "HIPAA privacy meets byod.," *Long-Term Living Contin. Care Prof.*, 2015.

[63] A. Meneghetti, "Challenges and benefits in a mobile medical world," *Health Manag. Technol.*, 2013.

[64] J. Free, "Real-world BYOD security BYOD security strategie from two distinct healthcare organizations.," *Health Manag. Technol.*, 2014.

[65] M. Hillier, "e-Exams with student owned devices: Student voices," in *Proceedings of the International Mobile Learning Festival 2015: Mobile Learning, MOOCs and 21st Century learning*, 2015.

[66] M. Hillier and A. Fluck, “Transforming exams-how IT works for BYOD e-Exams,” in *Proceedings ASCILITE2017: 34th International Conference on Innovation, Practice and Research in the Use of Educational Technologies in Tertiary Education*, 2017, pp. 100–105.
[67] T. K. Seow and S. K. A. Soong, “Students’ perceptions of BYOD open-book examinations in a large class: A pilot study,” in *Proceedings of ASCILITE 2014 - Annual Conference of the Australian Society for Computers in Tertiary Education*, 2014.
[68] B. Küppers, R. Zameitat, and U. Schroeder, “e-Assessment: Ensuring Equality of Treatment in a BYOD-Setting.” EUNIS Proceedings, 2018.
[69] B. Küppers and U. Schroeder, “Bring Your Own Device for E-Assessment - a Review,” *EDULEARN16 Proc.*, vol. 1, pp. 8770–8776, 2016, doi: 10.21125/edulearn.2016.0919.
[70] C. Engelhard and K. Kyeong-Ju Seo, “Going from obsolete to innovative: Empowering problem-based learning with online social media,” *Des. Probl. Instr. with Online Soc. Media, Inf. Age Publ. Charlotte, NC*, 2012.
[71] B. Collis and J. Moonen, “Web 2.0 tools and processes in higher education: Quality perspectives,” *EMI. Educ. Media Int.*, 2008, doi: 10.1080/09523980802107179.
[72] M. Mardis and N. Everhart, “From Paper to Pixel: The Promise and Challenges of Digital Textbooks for K-12 Schools,” 2013.
[73] P. Twining, “Redefining education: 1:1 Computing strategies in English schools,” *ACEC 2014 Now its Pers.*, 2014.
[74] J. Bailey, C. Schneider, and T. Vander Ark, “Funding the shift to digital learning: Three strategies for funding sustainable high-access environments,” *Digit. Learn. Now*, 2012.
[75] D. Cristol and B. Gimbert, “Academic Achievement in BYOD Classrooms,” *QScience Proc.*, 2013, doi: 10.5339/qproc.2013.mlearn.15.
[76] M. Sharples, “Disruptive devices: Mobile technology for conversational learning,” *Int. J. Contin. Eng. Educ. Life-Long Learn.*, 2002, doi: 10.1504/ijceell.2002.002148.
[77] K. Sangani, “BYOD to the classroom,” *Eng. Technol.*, 2013, doi: 10.1049/et.2013.0304.
[78] F. Kumar, “Analysis regarding the Bring Your Own Device (BYOD) policy and its influence on cyberbullying in the classroom.” 2015.
[79] P. W. Maus, “Determining the effect of bring your own device on cyberbullying incidents at a high school.” 2016.
[80] S. Zhang and D. Leidner, “Workplace cyberbullying: The antecedents and consequences,” *Soc. Issues Soc. Incl. Track*, 2014.
[81] K. C. Janssen and S. Phillipson, “Are we ready for BYOD? A systematic review of the implementation and communication of BYOD pograms in Australian schools,” *Aust. Educ. Comput.*, vol. 30, no. 2, 2015.
[82] M. Brodin, J. Rose, and R. M. Åhlfeldt, “Management issues for bring your own device,” *Proc. 12th Eur. Mediterr. Middle East. Conf. Inf. Syst. EMCIS 2015*, vol. 2015, pp. 1–2, 2015.
[83] R. E. Miller and J. Varga, “Benefits of Enabling Personal Handheld Devices in the Enterprise.” Intel Corporation, 2011.
[84] N. Singh and M. Phil, “B . Y . O . D . Genie Is Out Of the Bottle – ‘ Devil Or Angel ,’” *J. Bus. Manag. Soc. Sci. Res.*, 2012.
[85] N. Green, “On the move: Technology, mobility, and the mediation of social time and space,” *Inf. Soc.*, 2002, doi: 10.1080/01972240290075129.
[86] B. Kehoe, “BYOD - Proceed with caution,” *Hospitals and Health Networks*. 2013.
[87] R. Walters, “Bringing IT out of the shadows,” *Netw. Secur.*, 2013, doi: 10.1016/S1353-4858(13)70049-7.