International Journal of Future Generation Communication and Networking
Vol.14, No. 1, (2021), pp. 3048–3056

A Detailed Review on Security Issues of Bring Your Own Devices (BYODs)

Sarita Sushil Gaikwad, Ph.D. student , Kalinga University, Raipur.
Dr. Aparna Junnarkar, Ph.D. Co Guide , Kalinga University, Raipur.

ABSTRACT

In recent days, Bring Your Own Device (BYOD) has turn out to be one of the most popular model for the enterprises that providing mobility and flexibility in work-places. The emergence of latest innovations and features of mobile devices makes them integral part of every aspect of everyday business activities. Furthermore, these mobile networks are now well integrated with the Internet, personal devices can be used in BYOD to raise employee satisfaction while lowering system costs. In comparison to computers and computer networks, mobile devices are not well secured, and users pay less attention to security updates and solutions. As a result, as workers use their own mobile devices to access an organization's data and systems, mobile security has become a critical problem in BYOD. However, because of new threats and resource constraints on computing machines, it's difficult to trust these devices with access to sensitive proprietary data. As a result, the possible attacks (e.g. Advanced Persistent Threat (APT) and malware) of BYOD and a taxonomy of BYOD attacks are presented in this article. Also, we present a summary of the current state of BYOD protection in this article and address it.

KEYWORDS: BYOD, Security, BYOD Attacks, Malwares, Advanced Persistent Threat and Secure BYOD.

1. INTRODUCTION

With increased usage of digital technology, one thing is clear that ‘BYOD’ simply cannot be ignored & is here to stay. New companies are using ‘BYOD’ as the foundation for developing their network infrastructure. A large number of growing organizations are allowing employees to purchase & use their own devices at the workplace. Smartphones & Tablets have provided unprecedented level of flexibility, thus leading to IT consumerization. Therefore, when an employee purchase their own devices, the company can save a lot of their IT & hardware related costs. ‘BYOD’ means comfort for workers and increased productivity for the organizations that implement a well-defined ‘BYOD’ plan. A person sitting with their digital device may check their emails, Twitter account, update Outlook calendar and may even make a video call. ‘BYOD’ also provides a lots of benefits for businesses like: less time offline for workers would mean project work moves forward as fast pace and important business decisions are no longer restricted to 9-to-5 timings. While the organizations and employees have a lot to work on ‘BYOD’ part, digital technology devices like – tablets, smartphones, laptops, PCs etc. that coworkers move & work around are here to stay.

The competitive setting of today’s world has rendered the working and personal life of individuals to be interconnected. One can manage his/her personal life while working and vice versa. With a growing workload, an employee is often tied down with deadlines even after working hours. This complicates the work-life balance of the employee, thus causing dissatisfaction. Some employees prefer to work in the comfort of a place of their choosing. However, traditional working systems do not allow for such flexibility, causing grievances among employees. One of resolutions for this issue comes in terms of Bring Your Own Device (BYOD) idea, i.e., a method whereby employee devices are connected to their company’s network for routine tasks [1] – [6]. In short, the company allows its worker to equip themselves with gadgets used for their jobs-related purposes. This notion was first introduced in the early 20th century and brought benefits for employees and companies in numerous fields. The BYOD approach has been employed in various domains, including the medical field [7] – [9], higher education [10], [11], and healthcare sectors. The adoption of new technologies or principles is driven by the benefits that such developments offer. This notion hence provides a more effective solution for the users and the administrators. Among the identified benefits of this approach are: lower procurement costs, greater workplace flexibility, higher job satisfaction, a more empowered working environment, better productivity, and reduced working hours. Nonetheless, the approach also suffers from several limitations: activities not related to work, core competency loss, privacy issues, and rapid technological evolution. These benefits and limitations occur in all

ISSN: 2233-7857IJFGCN

domains and vary according to the fields. The adoption of new technologies or concepts often comes with its pros and cons. Technology is beneficial when proper guidelines are followed. As BYOD application had found to be rising currently, amount of research in perspective of their security is comparatively less. Hence in this study we will perform investigation on security issues pertaining to BYOD technology as well as its shortcomings.

2. LITERATURE REVIEW

Several studies examined the concept of BYOD in the context of business [12] – [14]. The study's findings revealed that a company achieved increased earnings of 0.002 Billion USD when 1,000 of its employees undertook the BYOD approach. The study also revealed that when an employee uses his/her own devices, unnecessary work issues can be reduced, including operating systems, hardware issues, network traffic, and new technology learning.

A similar study asserted the significant role of BYOD and cloud computing in providing and controlling information technology security today [15] – [17]. According to Kristine and Judith [18], the adoption of BYOD in the working sector improves the employees' work flexibility, adaptability, productivity, and commitment. These benefits underline the prevalence of BYOD across industries. The authors also asserted that BYOD could occasionally affect work activities negatively. With BYOD, there is a possibility that employees will spend time doing non-work related activities such as social networking. Therefore, this approach is not suitable for all fields of work.

Many studies investigated the threads and security issues related to BYOD [19] – [21]. Many studies and authors examined the tangible and intangible threads of BYOD; the former deals with device loss or theft while the latter deals with digital security issues such as virus and malware attacks [22] – [25]. Mahesh and Hooter et al. [26] highlighted the pervasiveness of the data generated from smart devices. Such data holds sensitive user information; hence, its loss due to theft or cyber attacks results in devastating consequences.

MobileIron[27] in their first series suggested about 8 components that will be helpful in adoption of a secure & scalable BYOD program. They are: Device choice, Sustainability, Trust Model, User experience & policy, Liability, Internal Marketing, Economics, and App Design & governance. 'BYOD' has been attractive mainly due to the increased usage of the tablets & smartphones – that have captured the majority of the consumer market. As per the reports of Wipro [28], the primal reason for rise in 'BYOD' is due to the proliferation of smartphones and IT consumerization. The enterprises are embracing BYOD due to the gainful benefits like improved user experience, increased productivity, and the anytime, anywhere availability of data & applications, and cost-reduction in hardware and management. Information security has always been a major concern when it comes to accessing corporate data & systems. It becomes difficult in believing such devices by providing access to them for sensitive proprietary related data because of many latest attacks and restrictions on resources of these gadgets are quite evident.

Ghosh, A. et al [29] gave measures for mobile security like determining responsibilities and roles in securing and managing device, testing application, registering mobile devices to be implimented in these devices, updating security settings & training employees regarding security issues. Therefore, with the increased usage of digital technologies, 'BYOD' awareness becomes important. Some organizations have adopted 'BYOD' but many organizations are still on the deciding mode or have not yet adopted. 60% of commercial establishment have not yet accepted BYOD, but are under consideration according to survey concluded by Schulze [30]. Whereas 24% are practically working on infrastrure, procedures and policies for BYOD, Only 10% of non-adopters are opting out of it.The primal reason for the non-adopters of 'BYOD' is the security issue. With digital revolution, the future is all about under-standing 'BYOD' and

ISSN: 2233-7857IJFGCN

include it in the organization's policy making. In this dynamic worldCognizant Co. [31] in their report mentioned that it is necessary to adopt BYOD concept for all companies for their survival.Many issues challenges like support systems, data protection, security and cost for BYOD were faced by them.

3. BYOD ATTACK AND SECURITY CONCERNS

Potential attack vectors could be used against personal devices in a BYOD scenario, in order to proposed solution to constrict issues in BYOD

3.1. Lost or stolen mobile devices

Mobile devices are very easy and prone to lose or get stolen as these issues cannot be changed or minimize as it involves human behaviour. Almost every individual saves quite large amount of personal information and company sensitive information related to their jobs on these mobile devices. With respect to loosing or stealing of mobile devices are concern, roughly 1.3 million mobile devices were stolen every year in United Kingdom alone [32]. Apart from this fact, many United States corporation losses them by means of theft like 640 laptops and 1075 smartphones every week [32]. Therefore quite large amount of important data is lost with these lost devices. Even after such a great data lost in these scenarios nothing seriously is done in protecting organization data or client based data on these personnel gadgets. Hence,substantial amount of attack effects security concern of BYOD with these stolen or lost hand held devices.

3.2. Eavesdropping

With Common Vulnerabilities and Exposures (CVE) holes and probable infection through eavesdropping software hand held devices are very much prone. With WIFI connectivity additionally, Phishers may operate through cellular networks and can eavesdrop along these network, which can put organizations vital information at risk [33]. In this same manner, if any kind of information like e-mail messages or passwords send with WiFi or a LAN connectivity it become more easy to eavesdropping posing security threat [33].

3.3. SQL injection

Code injection technique is used by SQL injection for targeting websites and applications, thereby inserting data-stealing malware software. Because of BYOD trend in workplace, SQL injection attack were found to be as an epicentre of many data breaches previously. 42 per cent of all breaches are from source of SQL injections as per Security Week research [34]. the root causes of more difficult. Due to widening trend for workforce in using their BYOD in workplace, it become very difficult in determining root cause of SQL injection attack.

3.4. Advanced Persistent Threat (APT)

A set of stealthy and continuous hacking processes is APT [35]. For buisnesses APT usually targets companies or in some cases nations. Apart from other instant attacks, APT procedures needs a high level of concealing on a long span of time [36]. Advanced, persistent and threat are three main constituents of APT. Whenever attackers identifies anomalous high traffic on networks APT attacks against end users. BYOD systems may alllowunverified and unauthorized entities in granting access to companies vital servers and facilities like no encryption of company data in mobile devices that can give chance for an attacker in conducting APT attack leading to security threats.

3.5. Company and client's data privacy

Personally owned device raises legal concerns around data privacy as Monitoring and accessing data applications are installed on it .Various problems takes place as major aim of BYOD is that workers owns and to some extend supports and maintains personal devices. It is very difficult for organizations to ensure that company or client‘s data is not percolated to nonemployees like personal relationships like friends and family members who has access to these devices. Therefore, information security becomes and important attack in case workforce makes use of

ISSN: 2233-7857IJFGCN

BYODsystems for their working purposes either during nonwork hours or working hours.

3.6. Social Engineering

Gathering of sensitive or confidential information with psychological manipulation is method of Social engineering. To acquire and hold sensitive and valuable data is an objective for attackers in carrying out social engineering. Phishing, baiting and virus hoaxes are technique of social engineering in BYOD atmosphere. To carry out social engineeringunauthorized mobile app and malicious link are common attacking vector that were used by attackers for data manipulations.

3.7. Malware

Since last couple of years it is evident that growth of malware in mobile devices has risen tremendously, becoming one of largest risk for organization and corporation using BYOD environment. To transmit and release their payloadVarious attacking vectors are available for malwares, specifically in BYOD environment.

3.8. Attack with Secure socket layer

An attack that focus on exploring and breaching vulnerabilities of network protocol is known commonly as secure Socket layer attack. For such attacks SSL/TLS is usual protocol that are targeted by attacker. To demonstrate an objective and purpose of these attackHeartbleed is most acceptable case study in this regards. Almost One third of username along with password that were stored in different servers in this world were hacked because of outbreak of Heartbleed. These attack leads to increase risks to non secured mobile device that are equipped with vital corporate information in BYOD systems. For instance there wer an estimated of 50 million users that got affected by Android version 4.1.1 which was vulnerable to Heartbleed [37] in this outbreak.

3.9. Man-in-the mobile

For mobile version of man in the middle, man in the mobile is a latest term used. Man in the mobile attack can be carried out easily if malicious spyware or keyloggergets applied into any unsecured mobile devices. For instance ,zitmo (zeus in mobile) may be implemented Andoird devices, and can intercept and read SMSes. By using this type of attackSensitive and delicate information likemTan can be very easily recovered by attackers.

For any corporate organizations information is an important and critical parts as BYOD has risen amount of expensive security incidents for data. We found some important facts related to BYOD in loosing company or client’s information.Sensitive corporate data and client information can be easily transmitted and gets vanishes. Increasing numbers of mobile devices almost 93% of them areconnecting to corporate networks [38]. As soon as BYODs grows quickly thereby producing issues for corporate world. Customer personal information on mobile devices creates data protection risks as reported that 53 % of users maintain their sensitive customer information on mobile devices [38]. In an incident related to mobile security breaching 94% indicate lost or stolen customer information is critically concerning [38]. Malware infections (47 percent),unauthorized access to company data and systems (65 percent) and Loss of client or company information (75 percent) are the three major security concerns [39]. Figure 1 depicts overall survey result as shown below

ISSN: 2233-7857IJFGCN

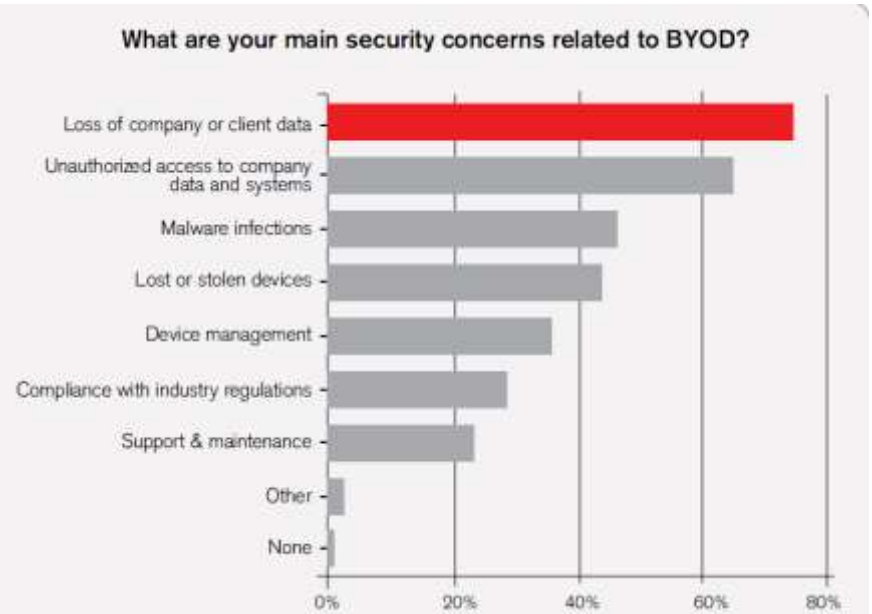

Figure 1 BYOD's security concern a survey result [39]

Figure 2 explains Owasp listing of top 10 mobile securityrisks .Effects of each respective risks as mentioned will be discussed in details in section followed.

Figure 2: Major 10 mobile security risks of OWASP[40]

• ***Server side control not strong***

Such vulnerability directs towards technical effects of related risks thatadversary is misusing through mobile device. As an example, a Cross-SiteScripting (XSS) vulnerability via mobile device can be easily exploited by an adversary [40].

• ***Data storage not secure***

Data loss may occurs if there is insecure data storages, as a best case for standalone user whereas for worst case scenario formany users. Transaction histories,authenticationtokens, user name, cookies, passwords and location data are part of Common valuable pieces of data sets that are stored or any confidential data [40].

• ***Transport layer protection not sufficient.***

ISSN: 2233-7857IJFGCN

Such drawback discloses risk of an individual user's information and can lead to hijacking or account theft. Entire site could be exposed if adversaryintercepts an admin account. Phishing and MITM attacks can be facilitated by Poor SSL setup[40].

• Data leak Unintended

Such kinds of risk may involves in following technological implications:forensic tools,modified apps or extraction ofapplications' sensitivedata through mobile malware, [40].

• Low grade of authentication and authorization

Authorization failures can bring up basicAuthentication malfunctions as well. Solution is not capable in verifying user's identity ifauthentication controls fail. Such identities are linked to usersassociated permissions, roles and responsibilities. Whenever an attacker tries to anonymously process sensitive functionality, it will indicate that underlying code is not authenticating access permissions ofparticular user generating request for any action [40].

• Discontinuous cryptography

These vulnerability leads in unauthorized recovering of important and critical data throughmobile devices.

• Client side injection

If an application is dealingwith multiple user account at same time executing on a single application or a shared device or paid-for content then injection attacks such as SQL Injection on mobile devices can be severe in operations [40].Rest of injection points are aimed at providing overflow application constituents, however there remains very few chances toget a high effected outcome due to managed code security of applicationlanguages.

• Sources of untrusted inputs in Security decision

Whole security model or architecture of organization will be at risk if Security decisions are executed through untrustworthyinputs . As predicting untrustworthy inputs is difficult in these scenarios as users which are inbound are provided ease in accessing organizations as well as clientsinformations.

• Session handling Improperly

If session token is unintentionally shared to adversary throughout a subsequent interchange of information between mobile app and backend servers improper session handling takes place [40]. In worst case conditions, adversary is concealing its identity and behaves like an administrative user and putting uprequest for administrative rights which is dangerous in for data securities.

• Binary protection absence

From adversary point of view binary protections does not allowit to changebasicbehavior or code todisable or add additional functionality. Such scenarios takes place when an apptransmit, stores, or execute personally identifiable information (PII) or other important and sensitivedata such as credit card credentials or passwords [40]. Changes in Code generally occurs in terms of insertion orrepackaging of malware insidepreexisting mobile applications.

4. TAXONOMY OF BYOD ATTACKS

In previous section various type of attacks have been explained. BYOD attacks taxonomy is grouped in security and components attacks. User,network, software, physical and web are included in components. Whereas, active attacks, passive attacks and privacy attacks are done for security attacks .Entire BYOD attacks taxonomy is provided in Table 1 as follows.

ISSN: 2233-7857IJFGCN

Table 1: BYOD attacks Taxonomy

Components	Security Attacks		
	Active Attacks	Passive Attacks	Privacy Attacks
User	Man-in-the-mobile Social engineering	Eavesdrop-ping	Data privacy for company and client
Network	SSL attack		
Software	Malware APT		
Physical		Lost or stolen mobile devices	
Web	SQL injection		

5. A Secure BYOD Model

The framework of the secured authentication model was explored and onboarding was done securely [41] of BYOD internal users. The multi-factor authentication model with a Certicate-based Hybrid model of authentication was one of the successful models with 3 tier captcha [42]. Apart from this secure communication mechanism with a dual-factor authentication method has been explored using Scyther Tool and the dual-factor authentication mechanism was tested for automatic verification tools with a secured approach in IoT [43] environment. While BYOD is in LAN secured model of onboarding was also explored using 802.1x authentication security control [44] mechanism.

Encryption of corporate data in BYOD was a successful model to secure corporate data [45]. End to end encryption and cryptographic method of network security is an option in recent research in 2019 also a secured model [46]. During remote access services Denial-of-Service Attack (DDoS) attack network traffic gets congested in remote site traffic authentication traversingwas critical aspect [47] which was explored and mitigation with IDS/IPS.

6. CONCLUSION

Bring Your Own Devices (BYODs) are widely used by enterprisers and workers because they have a range of benefits. BYOD protection models currently only include a sandbox for mobile devices and communication, with features including data and communication encryption, containerization, application access, and authentication. Since these primary solutions rely on rules to monitor mobile devices, they are unable to detect mobile malware in the sophisticated form of mobile Botnets. We have addressed a survey of security issues in the BYOD environment in corporate and organisational settings in this article. The potential attacks that could occur in a BYOD setting are described and addressed, followed by classification. ATP and malware attacks are the two most common types of attacks. Also, we have presented a detailed literature review and survey that have performed. In the near future, we will implement the proposed solution and evaluate it in a real BYOD environment to evaluate the performance of our proposed solutions. We will incorporate the solution and test it in a real BYOD environments in the near future.

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.

ISSN: 2233-7857IJFGCN

[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, p. p. 65 – 70, 2013, doi: 10.19030/rbis.v17i2.7846.
[13] K. Downer and M. Bhattacharya, "BYOD security: A new business challenge," in *Proceedings - 2015 IEEE International Conference on Smart City, SmartCity 2015, Held Jointly with 8th IEEE International Conference on Social Computing and Networking, SocialCom 2015, 5th IEEE International Conference on Sustainable Computing and Communications, SustainCom 2015, 2015 International Conference on Big Data Intelligence and Computing, DataCom 2015, 5th International Symposium on Cloud and Service Computing, SC2 2015*, 2015, doi: 10.1109/SmartCity.2015.221.
[14] A. Ghosh, P. K. Gajar, and S. Rai, "Bring Your Own Device (Byod): Security Risks and Mitigating Strategies," *J. Glob. Res. Comput. Sci.*, 2013.
[15] Gartner, "Gartner IT Glossary," 2012. [Online]. Available: https://www.gartner.com/en/information - technology/glossary/consumerization. [Accessed: 20 - Jan - 2018].
[16] E. Semenikhina, M. Drushlyak, Y. Bondarenko, S. Kondratiuk, and N. Dehtiarova, "Cloud - based service geogebra and its use in the educational process: The BYOD - approach," *TEM J.*, 2019, doi: 10.18421/TEM81 - 08.
[17] Ps. SreeLaxmi, Kk. Bharathi, and Chm. Pushpa, "Role of Mobile Cloud Applications and Challenges in BYOD," *Int. J. Comput. Tech.*, 2015.
[18] K. Dery and J. MacCormick, "Managing mobile technology: The shift from mobility to connectivity," *MIS Q. Exec.*, 2012.
[19] B. Markelj and I. Bernik, "Mobile devices and corporate data security," *Int. J. Educ. Inf. Technol.*, 2012.
[20] B. Morrow, "BYOD security challenges: Control and protect your most sensitive data," *Netw. Secur.*, 2012, doi: 10.1016/S1353 - 4858(12)70111 - 3.
[21] B. Alotaibi and H. Almagwashi, "A Review of BYOD Security Challenges, Solutions and Policy Best Practices," in *1st International Conference on Computer Applications and Information Security, ICCAIS 2018*, 2018, doi: 10.1109/CAIS.2018.8441967.
[22] M. Mahinderjit Singh, S. Sin Siang, O. Ying San, N. H. A. HassainMalim, and A. R. MohdShariff, "Security Attacks Taxonomy on Bring Your Own Devices (BYOD) Model," *Int. J. Mob. Netw. Commun. Telemat.*, 2014, doi: 10.5121/ijmnct.2014.4501.
[23] F. Li, C. T. Huang, J. Huang, and W. Peng, "Feedback - based smartphone strategic sampling for BYOD security," in *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, 2014, doi: 10.1109/ICCCN.2014.6911814.
[24] Z. M. Zain, S. H. Othman, and R. Kadir, "Security - based BYOD risk assessment metamodelling approach," in *Proceedings ot the 21st Pacific Asia Conference on Information Systems: "'Societal Transformation Through IS/IT'", PACIS 2017*, 2017.
[25] M. I. Ali and S. Kaur, "BYOD secured solution framework," *Int. J. Eng. Adv. Technol.*, 2019, doi: 10.35940/ijeat.F8202.088619.
[26] 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.
[27] Z. M. Zain, S. H. Othman, and R. Kadir, "Security - based BYOD risk assessment metamodelling approach," in *Proceedings ot the 21st Pacific Asia Conference on Information Systems: "'Societal Transformation Through IS/IT'", PACIS 2017*, 2017.
[28]. MobileIron. (2011). BYOD Strategies Chapter 1. [online] Available at: http://www.webtorials.com/main/resource/papers/mobileiron/paper1/byod_part_1.pdf [Accessed 12 Feb. 2016]

ISSN: 2233-7857IJFGCN

[29]. Ghosh, A., Gajar, P. K., &Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. Journal of Global Research in Computer Science, 4(4), 62 - 70.
[30]. M. I. Ali and S. Kaur, "BYOD secured solution framework," *Int. J. Eng. Adv. Technol.*, 2019, doi: 10.35940/ijeat.F8202.088619
[31]. Cognizant, (2014). Making byod work for your organization. Banglore: Whitepaper
[32] SYBASE, "Mobility Advantage: Why Secure Your Mobile Devices? White Paper", February 2013.
[33] Jessica Keyes, "Bring Your Own Devices (BYOD) Survival Guide", CRC Press Taylor & Francis Group, Boca Raton, 2013
[34] Brian Prince (16th April 2014), SQL Injection Breaches Take Months to Uncover and Fix: Survey, [Online] Available: http://www.securityweek.com/sql-injection-breaches-take-months-uncover-andfix-survey, Last Accessed Date: 23 May 2019.
[35] Dell Secure Works, "Anatomy of an Advanced Persistent Threat (APT)", 31 March, 2011.
[36] Command Five Pty Ltd, "Advanced Persistent Threats: A Decade in Review", June 2011.
[37] Why heartbleed could be much worse for android user [TOnline] http://bgr.com/2014/04/16/ heartbleedandroid-4-1-1-jelly-bean/ Accessed date: 17/5/2019
[38] Check Point Software Technologies Dimensional Research, "The Impact of Mobile Devices on Information Security", June, 2013.
[39] Lumension Information Security, "2013 Survey Results of BYOD & Mobile Security", 2013.
[40] Owasp Mobile Security project https://www.owasp.org/index.php/OWASP_Mobile_Security_Project Accessed Date : 20/5/2019
[41]. E.A. Lee, Cyber physical systems: Design challenges, in: 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), May2008, pp.363 – 369.
[42]. C.W. Tien, J.W. Liao, S.C. Chang, S.Y. Kuo, Memory forensics using virtual machine introspection for malware analysis, in: 2017 IEEE Conference on DependableandSecureComputing, Aug2017,pp.518 – 519.
[43]. J. Gosling, B. Joy, G. Steele, G. Bracha, A. Buckley, The java virtual machine specification-javase8edition,feb.2015.
[44]. G.Grispos, W.B.Glisson, K.K.R.Choo, Medical cyber - physical systems development: A forensics - driven approach, in: 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), July2017, pp.108 – 113.
[45]. P. K. Gajar, A. Ghosh, and S. Rai, ``Bring your own device (BYOD): Security risks and mitigating strategies," Tech. Rep., 2010, p. 9.
[46]. K. Joshi, M. Pathak, S. Jose, S. Dahiya, and S. Jose, ``(71) applicant: Gigamon Inc., Santa Clara, CA (US)," Tech. Rep., p. 18.
[47]. M. M. Singh, S. S. Siang, O. Y. San, N. H. A. H. Malim, and A. R. M. Shariff, ``Security attacks taxonomy on bring your own devices (BYOD) model," Int. J. Mobile Netw. Commun. Telematics, vol. 4, no. 5, p. p. 117, Oct. 2014, doi: 10.5121/ijmnct.2014.4501.

ISSN: 2233-7857IJFGCN