A Systematic Review Of Bring Your Own Device (BYOD) Authentication Technique

Fara Jamal¹, Mohd. Taufik¹ Abdullan, Azizol Abdullan¹ and Zurina Mohd. Hanapi¹

¹Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

f4ra.jamal@gmail.com,

Abstract. This article provides a systematic review of Bring Your Own Device (BYOD) authentication technique. The review main goal is to identify the existing BYOD authentication technique and to categorize the technique according to BYOD security threat as well as to analyze the technique limitation. The review result shows that there are 25 authentication techniques proposed across both industry and academic areas to fit into BYOD implementation to enhance the security in preventing and detecting data leakage in the organization. It is hoped that the proposed BYOD authentication solution can help organizations to minimize the number of cases in data leakage while allowing the BYOD concept.

1. Introduction
The term Bring Your Own Device or BYOD has started being discussed since 1990 but only being widely used in 2011 [1]. Many organizations implement BYOD in order to enhance their computing resources, especially in terms of hardware. It is also believed that BYOD actually increases employee productivity. Mobile devices are being used widely in the office, whether the organization implementing BYOD or not. In 2018, there are about 10 billion devices available which means every person in the world will have more than one device and 69% employees use personal mobile devices to connect to corporate network even in a non-BYOD organization [2].

As many organizations find BYOD technology brings a lot of benefit to the employees as well as the organizations, they also worry about the disadvantages and the challenges they are facing. The main security concern is not about the devices or the information inside the organization, but it’s about controlling the access from the user and the device to the organizational information, and the increased exposure of the enterprise network to malware due to the lack of control and visibility of mobile devices [3]. Organization must make sure that when a user uses their personal device to access organization information, the device must meet some standard of authentication [4] as well as protection against malware to prevent from data leakage.

Therefore, the purpose of this study is to identify the existing authentication technique. The technique will be categorized according to security threat related to BYOD. Based on more than 100 journals and conference papers read, the top threat that have been discussed by previous researchers are the security attack (32%) followed by malware (29%). Data leakage is the third main concern which is 14% and followed by loss or stolen device (12%). Only 5% researchers talked about DDOS attack and 1% discussed on the unauthorized software and bandwidth problem as in Figure 1. Table 1
Figure 1.: BYOD Security Threat

Table 1: List of researchers

| OD Security Threat                        | Author                                                                 |
|-------------------------------------------|------------------------------------------------------------------------|
| Loss/ Stolen of Device                    | [5]; [6]; [7]; [8]; [9]; [10]; [11]; [12]; [13]; [14]; [15]; [16]; [17]; [18]; [19]; [20]; [21]; [22]; [23]; [24]; [25]; [26]; [27]; [28]; [17]; [29]; [30]; [31]; [32]; [33]; [5]; [34]; [35]; [36]; [37]; [38]; [6]; [39]; [40]; [41]; [42]; [43]; [44]; [45]; [46]; [47]; [48]; [49]; [50]; [51]; [52]; [53]; [54]; [55]; [8]; [56]; [57]; [58]; [59]; [10]; [60]; [61]; [12]; [62]; [14]; [63]; [64]; [65]; [66]; [25]; [67]; [68]; [18]; [69]; [70]; [21]; [71]; [72]; [73]; [74]; [75]; [22]; [23]; [76]; [77]; [78]; [79]; [80]; [81]; [82]; [83]; [84]; [27]; [28]; [79]; [85]; [86]; [87]; [31]; [88]; [5]; [34]; [37]; [89]; [39]; [90]; [91]; [92]; [93]; [94]; [95]; [44]; [46]; [41]; [96]; [50]; [97]; [98]; [53]; [7]; [56]; [58]; [10]; [99]; [61]; [64]; [65]; [18]; [21]; [71]; [77]; [81]; [82]; [79] |
only articles in peer-reviewed journals and reputable conferences shall be addressed. The remaining sections are as follows; review method, finding, discussion and conclusion.

2. Review Method
This section will explain the processes of Systematic Literature Review (SLR) based on guidelines by [117], [118] and [119]. It comprises of six subsections which are; SLR question, data source, search strategy, study selection, and inclusion and exclusion criteria.

The SLR guideline consists of three main phases which are planning the review, conducting the review and reporting the review phase. The detailed steps involve in every phases are shown in Figure 2.

![Figure 2: SLR Guideline](image)

2.1. Research Question
Research question is an important part when conducting a systematic review because it is the guideline for the entire process of the study. The research questions structure in this article used PICO paradigm which also implemented in [120]. PICO is a short form for the words of population, intervention, comparison, and outcome. The research questions (RQ) are addressed in this article as follows:

| Criteria      | Research Question                                                                 | Purpose                                                                 |
|---------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Population    | R1 : How many research articles related to BYOD authentication had been produced from 2013 to 2018? | To analyze how many articles had been produced in this study starting from year 2013 until 2018, with inclusion of all topic area in BYOD authentication |
| Intervention  | R2 : What are the techniques or methods used for BYOD authentication?               | To understand the techniques or method used by the researchers for their study. |
| Comparison    | R3 : What are the BYOD security threat that the technique try to solve?             | To define the technique used in the experiment are the best method to solve which type of security threat in BYOD. |
| Outcomes      | R4 : What are the limitations of the study?                                        | To identify any limitation exist for each technique by the researcher    |
2.2. Search Process
This section explains about the process used to search for the related works.

a. Data Source. For this study, published papers were searched from nine online databases as data sources which are IEEE Explorer, Emerald, Ethos (UK Thesis), SpringerLink, ScienceDirect, Scopus, Australian Digital Thesis (ADT), ProQuest (USA Thesis) and Taylor & Francis.

b. Search strategy. The initial search string were ("BYOD Authentication Technique"), (BYOD Authentication Technique), (BYOD AND Authentication), (Authentication AND Technique), ("BYOD Authentication Method"), (BYOD Authentication Method), (Authentication AND Method), ("BYOD Authentication Mechanism"), (BYOD Authentication Mechanism), (Authentication AND Mechanism), ("BYODAuthentication tools"), (BYOD Authentication tools), (Authentication AND tools), ("BYOD Authentication framework"), (BYOD Authentication framework), (Authentication AND framework), ("BYOD Authentication Assessment"), (BYOD Authentication Assessment), (Authentication AND Assessment), ("BYOD Authentication Architecture"), (BYOD Authentication Architecture), (Authentication AND Architecture), ("Bring Your Own Device Authentication Technique") and (Bring Your Own Device Authentication Technique). The search string was executed in the digital libraries based on title, abstract and metadata.

c. Study Selection. This step ranks the source of the articles from the highest ranking to the lowest based on the priority. The highest ranking is journals, followed by conferences, thesis reports, book chapters, magazine articles, technical reports and proceedings.

d. Inclusion and Exclusion Criteria. This review targeted peer reviewed articles published between January 2013 until October 2018. Only articles that are journal, conference paper, thesis report and book chapter that written in English language were included. The search included articles that meet the research question defined. Any article which is not related to BYOD authentication will be excluded from the selection process. However, the article still can be selected for review if the work is applicable to the BYOD authentication area.

3. Result
The initial phase of the search process identified 254,614 studies using the search term defined. Table 3 shows the summary of search result from the search process which displayed the number of publications found based from each digital library database and the number of publications found from each key word.

| Library | IEEE Explorer | Ethos (UK Thesis) | Springer Link | Science Direct | Scopus | Australian Digital Thesis (ADT) | ProQuest (USA Thesis) | Taylor & Francis |
|---------|---------------|-------------------|---------------|----------------|--------|--------------------------------|-----------------------|------------------|
| "BYOD Authentication Technique" | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| BYOD Authentication Technique | 2 | 11 | 0 | 170 | 17 | 5 | 0 | 0 |
| BYOD AND Authentication Technique | 25 | 11 | 0 | 262 | 197 | 38 | 0 | 0 |
| BYOD Authentication AND Technique | 152 | 3068 | 253 | 17324 | 13094 | 11856 | 0 | 0 |
| "BYOD Authentication" | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Method" | BYOD Authentication Method | BYOD AND Method "BYOD Authentication Mechanism" | BYOD Authentication Mechanism | BYOD Authentication AND Mechanism "BYOD Authentication tools" | BYOD Authentication tools | BYOD Authentication AND tools "BYOD Authentication framework" | BYOD Authentication framework | BYOD Authentication AND framework "BYOD Authentication Assessment" | BYOD Authentication Assessment "BYOD Authentication Architecture" | BYOD Authentication Architecture "Bring Your Own Device Authentication Technique" |
|---------|---------------------------|-----------------------------------------------|-------------------------------|-------------------------------------------------------------|-------------------------|---------------------------------------------------------------|-------------------------------|---------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------|
|         |                           |                                               |                               |                                                             |                         |                                                              |                               |                                                              |                                                              |                                                              |
|         | 6                         | 8                                             | 0                             | 47                                                          | 141                     | 7                                                             | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 254                       | 2895                                         | 499                           | 19356                                                      | 20297                   | 17710                                                        | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 0                         | 0                                             | 0                             | 0                                                          | 0                       | 0                                                             | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 5                         | 6                                             | 0                             | 35                                                          | 98                      | 7                                                             | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 4772                      | 1998                                         | 167                           | 14372                                                      | 12999                   | 9076                                                        | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 0                         | 0                                             | 0                             | 0                                                          | 0                       | 0                                                             | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 0                         | 9                                             | 0                             | 41                                                          | 146                     | 2                                                             | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 1388                      | 2595                                         | 195                           | 11,754                                                     | 10160                   | 3963                                                        | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 0                         | 0                                             | 0                             | 0                                                          | 0                       | 0                                                             | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 6                         | 9                                             | 0                             | 29                                                          | 97                      | 8                                                             | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 2818                      | 2077                                         | 379                           | 12402                                                      | 6909                    | 4071                                                        | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 0                         | 0                                             | 0                             | 0                                                          | 0                       | 0                                                             | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 1                         | 7                                             | 0                             | 19                                                          | 79                      | 3                                                             | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 401                       | 2109                                         | 248                           | 3142                                                      | 6475                    | 1365                                                        | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 0                         | 0                                             | 0                             | 0                                                          | 0                       | 0                                                             | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 1                         | 5                                             | 0                             | 34                                                          | 100                     | 2                                                             | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 3918                      | 1106                                         | 95                            | 12398                                                     | 6347                    | 5634                                                        | 0                             | 0                                                             | 0                                                             | 0                                                             |
|         | 0                         | 0                                             | 0                             | 0                                                          | 0                       | 0                                                             | 0                             | 0                                                             | 0                                                             | 0                                                             |
Of these, 341 studies were found to be potentially relevant based on the screening of titles. The 341 papers were then categorized based on the abstract. We grouped the article into BYOD, Cloud Computing, Information Security, IoT, Mobile device and network security as bar chart in Figure 3.

The articles were then filtered according to the inclusion and the exclusion criteria before being accepted for the synthesis of the evidence. BYOD and mobile device categories were taken into further selection because BYOD is our main target and BYOD also related to mobile device. Mobile device authentication can be used in BYOD authentication. Then we excluded articles that present discussion only but does not present any new technique or novel approach. The remaining 60 papers were examined by looking first at the introduction. Finally, after reading the full articles, 26 studies were accepted for the synthesis of evidence. Figure 4 shows the detailed flow of the selection process.
4. Discussion
This section explains and discusses research questions in section 2.1.

4.1. **R1 : How many research articles related to BYOD authentication had been produced from 2013 to 2018?**

There are 25 articles that related to BYOD authentication had been produced from 2013 to 2018. Each year there are a number of publications published in the respective topic area as in Table 4. The articles are from impact factor journal, Scopus journal, conference and book chapter.

**Table 4: Articles that related to BYOD authentication**

| Library       | No of Articles | Journal                                                                 | Impact Factor  | Year |
|---------------|----------------|-------------------------------------------------------------------------|----------------|------|
| IEEE Explorer | 12             | 2018 8th International Conference on Electronics Information and Emergency Communication (ICEIEC) | conference     | 2018 |
|               |                | 2018 IEEE International Conference on Consumer Electronics (ICCE)       | conference     | 2018 |
|               |                | 2017 International Caribbean Conference on Devices, Circuits and Systems (ICCDCS) | conference     | 2017 |
|               |                | 2017 International Conference on Electrical and Information Technologies (ICEIT) | conference     | 2017 |
|               |                | 2016 IEEE/CIC International Conference on Communications in China (ICCC) | conference     | 2016 |
|               |                | 2016 IEEE First International Conference                                  | conference     | 2016 |

**Figure 4: Process of selection**

- Total studies identified based on search criteria: N = 254,624
- Total studies identified based on title: N = 390
- Total unduplicated studies: N = 342
- Total article related to BYOD & mobile device domain: N = 126
- Total article with new technique in BYOD & mobile device domain based on articles review: N = 60
- Article that met inclusion criteria: N = 25
- Study excluded at search criteria: N = 254,224
- Duplicate study excluded: N = 48
- Study excluded based on abstract, exclude article in cloud computing, cyber security, Information security, IoT and network security domain: N = 241
- Exclude article that does not present novel contribution or new technique: N = 66
- Studied excluded at full articles stage that not related to solve security threat: N = 35
4.2. **R2**: What are the techniques or the methods used for BYOD authentication?

| ID | Author | Title |
|----|--------|-------|
| F1 | [121]  | A system for detection of abnormal behavior in BYOD based on web usage patterns |
| F2 | [99]   | Analysis of BYOD security frameworks |
| F3 | [122]  | Cross-platform, secure message delivery for mobile devices |
| F4 | [57]   | Device-invisible two-factor authenticated key agreement protocol for BYOD |
| F5 | [123]  | Enterprise WiFi Hotspot Authentication with Hybrid Encryption on NFC-Enabled Smartphones |
| F6 | [124]  | Facial biohashing based user-device physical unclonable function for bring your own device security |
4.3. R3: What are the BYOD security threat that the technique try to solve?

Table 6: Implementation to solve security threat

| BYOD Security Threat | Technique try to solve |
|----------------------|------------------------|
| ID | Security attack | Malware | Data Leakage | Lost/stolen | DD OS | Unauthorized software | Unauthorized access | Bandwidth problem | Unauthorized access | Authorized access | unauthorized access | Malware | Lost device | Data leakage detection | document management |
|---|-----------------|---------|--------------|-------------|--------|----------------------|-------------------|-------------------|-----------------|-----------------|------------------|---------|-------------|-----------------------|---------------------|
| F1 | √ | √ | √ | X | X | X | √ | √ | √ | X | X | X |
| F2 | X | X | √ | √ | X | X | √ | √ | √ | X | X | X |
| F3 | X | X | √ | √ | X | X | X | √ | √ | √ | X | X | X |
| F4 | √ | X | X | X | X | X | X | X | X | X |
| F5 | X | X | √ | X | X | X | X | X | X | X | X | X |
| F6 | X | X | √ | X | X | X | X | X | X | X | X | X |
| F7 | X | X | √ | X | X | X | X | X | X | X | X | X |
| F8 | X | X | √ | X | X | X | X | X | X | X | X | X |
| F9 | X | X | √ | X | X | X | X | X | X | X | X | X |
| F10 | X | X | √ | X | X | X | X | X | X | X | X | X |
| F11 | X | X | √ | X | X | X | X | X | X | X | X | X |
| F12 | X | X | √ | X | X | X | X | X | X | X | X | X |
| F13 | X | X | √ | X | X | X | X | X | X | X | X | X |
4.4. **R4**: What are the limitations of the study?

| ID  | Limitation                                                                                                                                                                                                 |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| F1  | The technique are based on user behaviour pattern. It might need more time to learn user pattern to detect abnormal behaviour. The server processing speed and space also need to be high end to analyse the pattern especially in a big organization. |
| F2  | The solution only focus on authorize user                                                                                                                                                                   |
| F3  | Only focus on sending and receiving message using mobile device                                                                                                                                              |
| F4  | Focus on authenticating user and device and detect device location only.                                                                                                                                       |
| F5  | Focus only on connecting the device to the network. The key are stored in user device which can be stolen.                                                                                                     |
| F6  | The solution only focus on authenticating user and device without include other threat such as security threat and malware that might also lead to data leakage                                                    |
| F7  | Limited to health care service that used Hippocratic protocol. Not all device support NFC.                                                                                                                     |
| F8  | Focus only on authenticating the user not the device                                                                                                                                                           |
| F9  | The main focus only on authenticate the user. After the user already been authenticate, there is no more controlled implemented                                                                               |
| F10 | The technique focus on authenticating user based on the keystroke. It will be difficult to use this authentication technique when user used mobile phone because the keyboard is different base on the device         |
| F11 | The technique used mobile device management tool where it need to be install in the user device. The user might not want to install it and the agent might not support different type of OS in mobile device                      |
| F12 | User and device authentication information are stored in the server. If the server been compromised, user might not be able to be authenticate                                                                  |
| F13 | The solution only provide a framework for better manage BYOD environment but did not suggest any tool to implement.                                                                                             |
| F14 | The solution focus on detecting malware and security threat when user accessing the website but it cannot scan the user device before the user are allow to connect to the organization network                         |
| F15 | The technique used data mining to detect user behaviour to predict future action which required high end computing processing.                                                                                |
F16 Data are stored in the cloud which is prone to attack. It is also difficult to get information needed when there is a security incident happen for investigation since cloud usually manage by different provider.

F17 Focus on authenticate the device and limited to android device only.

F18 The technique secure the authentication based on network connection so the features are limited to unauthorized access and detect stolen device only.

F19 The present work does not include the influences of the surrounding conditions like light, noise, motion, in the selection process, which can be considered for more accurate decision.

F20 The authentication need to perform credential from the cloud which could take same time depend on the network connection.

F21 The technique focus on authenticating user based on the keystroke. It will be difficult to use this authentication technique when user used mobile phone because the keyboard is different base on the device.

F22 The solution did not scan for malware in the device and cannot detect if the device are lost or stolen.

F23 Focus only on authenticating user using context-based biometric.

F24 The offline mode only limited to authenticate the user only. To use all the features in the solution, the device need to connect to the server.

F25 The security is depends upon the security provided by hypervisor. The document management only separate data in the device but cannot manage data access from organization database.

5. Conclusion
From the review of BYOD authentication technique, it can be concluded that there is gaining research interest in this area. Starting from year 2013, there are increasing numbers of model and technique proposed by academic researchers. These techniques can be guidance for organization to implement safer BYOD environment. However, most of the techniques usually focus at user or device separately. BYOD needs to make sure both device and user can be trusted to access the environment. Conventional authentication technique such as knowledge-based, possession-based, biometric-based and multifactor authentication are prone to attack. Therefore, more powerful authentication is needed. Most of the authentication techniques need to store the authentication information (password, ID, public key) somewhere in order to be used by the authentication system. The problem of centralized storage is, it can be a single point of failure [142]. The current BYOD solutions discussed by previous researchers doesn’t have complete solution and are still insufficient to protect BYOD environment. Most of the solutions can only prevent but cannot detect data leakage cases. Without the ability to prepare proactively, the important and the relevant digital evidence may not be there when security incident occur. Realizing this gap, for future research, the researcher will focus on implementing BYOD access control that cover most of the problem in BYOD environment and use blockchain to secure the technique.

Acknowledgements
We acknowledge that this research received support from the GPIPS Grant GP-IPS/2018/9644000 awarded by Universiti Putra Malaysia to the Faculty of Science Computer and Information Technology.

References
[1] F. Jamal, I. Technology, I. Technology, A. Abdullah, I. Technology, and I. Technology, “BYOD Authentication Process (BAP) Using Blockchain Technology,” Adv. Res. Dyn. Control Syst., vol. 10, no. 11, pp. 166–172, 2018.
[2] Y. Wang, J. Wei, and K. Vangury, “Bring Your Own Device Security Issues and Challenges,” in The 11th Annual IEEE CCNC-Mobile Device, Platform and Communication Bring, 2014, pp. 80–85.
[3] Stephen Pao and M. Thorne, “BYOD Security: Expert Tips on Policy, Mitigating Risks, &
Preventing a Breach Meet Our Panel of Data Security Experts,” 2016. [Online]. Available: https://digitalguardian.com/blog/byod-security-expert-tips-policy-mitigating-risks-preventing-breach. [Accessed: 18-Sep-2018].

[4] F. Jamal, M. T. Abdullah, Z. M. Hanapi, and A. Abdullah, “Reliable Access Control for Mobile Cloud Computing (MCC) With Cache-Aware Scheduling,” IEEE Access, vol. 7, pp. 165155–165165, 2019.

[5] J. C. Sipior, J. Bierstaker, and J. Lee, “A Bring-your-own-device Case for Use in the Classroom,” vol. 41, 2017.

[6] A. V. Herrera, M. Ron, and C. Rabadao, “National cyber-security policies oriented to BYOD (bring your own device): Systematic review,” Iber. Conf. Inf. Syst. Technol. Cist., pp. 2–5, 2017.

[7] N. Fani, R. Von Solms, and M. Gerber, “A framework towards governing ‘Bring Your Own Device in SMMEs,,’” pp. 1–8, 2016.

[8] F. Moreira and A. C. Computing, “Strategies for minimizing the influence of the use of BYOD and Cloud in organizations: 4CM Model,” 2016.

[9] A. Tewari, P. Nagdev, and K. Israni, “BYOD: Usability,” vol. 6, no. 3, pp. 2810–2814, 2016.

[10] A. Mishra and K. Jani, “Comparative study on bring your own technology [BYOT]: Applications & security,” Int. Conf. Electr. Electron. Signals, Commun. Optim. EESCO 2015, 2015.

[11] D. T. Arregui, “Mitigating BYOD information security risks,” 2015.

[12] B. M. Gaff, “Byod? Omg!,” Computer (Long. Beach. Calif.), vol. 48, no. 2, pp. 10–11, 2015.

[13] A. B. Garba, J. Armarego, and D. Murray, “Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments,” J. Inf. Priv. Secur., no. April 2015, pp. 37–41, 2015.

[14] M. Ketel and T. Shumate, “Bring Your Own Device: Security Technologies,” 2015.

[15] T. Kim and H. Kim, “A system for detection of abnormal behavior in BYOD based on web usage patterns,” 2015 Int. Conf. Inf. Commun. Technol. Converg., 2015.

[16] C. J. Utter and A. Rea, “The "Bring your own device " conundrum for organizations and investigators: An examination of the policy and legal concerns in light of investigatory challenges,” vol. 10, no. 2, 2015.

[17] N. Zahadat, P. Blessner, T. Blackburn, and B. a. Olson, “BYOD security engineering: a framework & its analysis,” Comput. Secur., vol. 55, pp. 81–99, 2015.

[18] J. M. Chang, P. C. Ho, and T. C. Chang, “Securing bYOD,” IT Prof., vol. 16, no. 5, pp. 9–11, 2014.

[19] S. Earley and M. R. Lee, “From BYOD to,” no. October, pp. 16–18, 2014.

[20] A. French, C. Guo, and J. P. Shim, “Current Status, Issues, and Future of Bring Your Own Device (BYOD),” Commun. Assoc. Inf. Syst., vol. 35, 2014.

[21] M. M. Singh et al., “SECURITY ATTACKS TAXONOMY ON BRING YOUR OWN DEVICES (BYOD),” vol. 4, no. 5, pp. 1–17, 2014.

[22] H. Romer, “Best practices for BYOD security,” Comput. Fraud Secur., vol. 2014, no. 1, 2014.

[23] P. A. H. Sansurooh, Krishnum; Williams, “BYOD in ehealth: Herding cats and stable doors, or a catastrophe waiting to happen?,” 3rd Aust. eHealth Informatics Secur. Conf., 2014.

[24] J. M. Woodside and S. Amiri, “Bring Your Own Technology (BYOT) to Education,” Syst. Cybern. Informatics, vol. 12, no. 3, pp. 38–40, 2014.

[25] R. Afreen, “Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges,” Int. J. Emerg. Trends Technol. Comput. Sci., vol. 3, no. 1, pp. 233–236, 2014.

[26] 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.

[27] A. D. Rivera, G. George, P. Peter, S. Muralidharan, and S. Khanum, “Analysis of security controls for BYOD (bring your own device),” pp. 1–10, 2013.
[28] B. Tokuyoshi, “The security implications of BYOD,” *Netw. Secur.*, vol. 2013, no. 4, 2013.

[29] K. Johnson and T. DeLaGrange, “SANS Survey on Mobility/BYOD Security Policies and Practices,” no. October, p. 19, 2012.

[30] A. Scarfo, “New security perspectives around BYOD,” *Proc. - 2012 7th Int. Conf. Broadband, Wirel. Comput. Commun. Appl. BWCCA 2012*, pp. 446–451, 2012.

[31] N. Singh and M. Phil, “B . Y . O . D . Genie Is Out Of The Bottle – ‘ Devil Or Angel ,’” *J. Bus. Manag. Soc. Sci. Res.*, vol. 1, no. 3, pp. 1–12, 2012.

[32] Y. Wang, K. Streff, and S. Raman, “Smartphone Security Challenges,” pp. 52–58, 2012.

[33] P. K. Das, A. Joshi, and T. Finin, “App behavioral analysis using system calls,” *2017 IEEE Conf. Comput. Commun. Work. INFOCOM WKSHPS 2017*, pp. 487–492, 2017.

[34] K. Timms, “BYOD must be met with a wider appreciation of the cyber-security threat,” *Comput. Fraud Secur.*, vol. 2017, no. 7, pp. 5–8, 2017.

[35] B. A. Toperesu and J. P. Van Belle, “Organisational capabilities required for enabling employee mobility through bring-your-own-device concept,” *Bus. Syst. Res.*, vol. 8, no. 1, pp. 17–29, 2017.

[36] P. Li and L. Yang, “Management strategies of Bring Your Own Device,” *MATEC Web Conf.*, vol. 100, p. 02007, 2017.

[37] M. Mahinderjit, C. Wai, and Z. Zulkefli, “Security and Privacy Risks Awareness for Bring Your Own Device (BYOD) Paradigm,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 2, pp. 53–62, 2017.

[38] J. Zhang and W. Lou, “Which DRM grade could BYOD users employ? A differentiated DRM service between the cloud and mobile devices,” *2017 IEEE/ACM 25th Int. Symp. Qual. Serv. IWQoS 2017*, 2017.

[39] A. Taal, J. Le, A. Ponce de Leon, J. A. Sherer, and K. S. Jenson, “Technological and Information Governance Approaches to Data Loss and Leakage Mitigation,” *Comput. Sci. Inf. Technol.*, vol. 5, no. 1, pp. 1–7, 2017.

[40] P. Borges et al., “Towards a Hybrid Intrusion Detection System for Android-based PPDR terminals,” in *Proceedings of the IM 2017 - 2017 IFIP/IEEE International Symposium on Integrated Network and Service Management*, 2017, pp. 1034–1039.

[41] N. Tsalis, “Exposing security and privacy liabilities in modern browsers,” no. March, 2017.

[42] W. Campbell, “The Impact of the Internet of Things (IoT) on the IT Security Infrastructure of Traditional Colleges and Universities in the State of Utah,” Northcentral University, Arizona, 2017.

[43] T. Pereira, H. Santos, and I. Mendes, “Challenges and reflections in designing Cyber security curriculum,” *EDUNINE 2017 - IEEE World Eng. Educ. Conf. Eng. Educ. - Balanc. Gen. Spec. Form. Technol. Carriers A Curr. Challenge, Proc.*, pp. 47–51, 2017.

[44] T. Radwan, M. A. Azer, and N. Abdelbaki, “Cloud computing security: challenges and future trends,” *Int. J. Comput. Appl. Technol.*, vol. 55, no. 2, p. 158, 2017.

[45] R. K. Kulkarni, “Digital Forensics,” *Int. J. Emerg. Technol. Eng. Res.*, vol. 5, no. 4, 2017.

[46] A. Zeichick, “Enabling innovation by opening up the network,” *Netw. Secur.*, vol. 2017, no. 4, pp. 12–14, 2017.

[47] L. Reinfelder and Z. Benenson, “Exploring Security Processes in Organizations: The Case of Smartphones,” no. September, 2017.

[48] T. McGill and N. Thompson, “Old risks, new challenges: exploring differences in security between home computer and mobile device use,” *Behav. Inf. Technol.*, vol. 36, no. 11, pp. 1111–1124, 2017.

[49] D. Dang-Pham, S. Pittayachawan, and V. Bruno, “Investigation into the formation of information security influence: Network analysis of an emerging organisation,” *Comput. Secur.*, vol. 70, pp. 111–123, 2017.

[50] J. H. Cox, R. Clark, and H. Owen, “Leveraging SDN and WebRTC for Rogue Access Point Security,” *IEEE Trans. Netw. Serv. Manag.*, vol. 14, no. 3, pp. 756–770, 2017.
[51] X. Song and C.-H. Yang, “Mobile Device Management System Based on AOSP and SELinux,” 2017 IEEE Second Int. Conf. Data Sci. Cybersp., pp. 417–420, 2017.

[52] T. Yu, S. K. Fayaz, M. Collins, and V. Sekar, “PSI: Precise Security Instrumentation for Enterprise Networks,” Proc. NDSS 2017, 2017.

[53] R. E. Crossler, F. Bélanger, and D. Ormond, “The quest for complete security: An empirical analysis of users’ multi-layered protection from security threats,” Inf. Syst. Front., no. 0101, pp. 1–15, 2017.

[54] H. L. Feliciano-Torres, “USING INNOVATION DIFFUSION THEORY AND THE TECHNOLOGY ACCEPTANCE MODEL TO EVALUATE THE SECURITY OF WIRELESS MOBILE DEVICES AT A POST-SECONDARY INSTITUTION,” 2017.

[55] L. Meehan, C. Campbell, and K. Radhakrishnan, “Threat and Mitigation Awareness Based Upon a Model Network Scenario with BYOD Aspects,” vol. 9, no. 3, pp. 1765–1773, 2016.

[56] M. Olalere, M. T. Abdullah, R. Mahmod, and A. Abdullah, “Bring Your Own Device: Security Challenges and A theoretical Framework for Two-Factor Authentication,” Int. J. Comput. Networks Commun. Secur., vol. 4, no. 1, pp. 21–32, 2016.

[57] J. Ni, X. Lin, K. Zhang, Y. Yu, and X. S. Shen, “Device-invisible two-factor authenticated key agreement protocol for BYOD,” 2016 IEEE/CIC Int. Conf. Commun. China, ICCC 2016, 2016.

[58] B. R. Ogie, “Bring Your Own Device,” IEEE Consumer Electronic, no. january, 2016.

[59] A. Weeger, X. Wang, and H. Gewald, “IT Consumerization: BYOD-Program Acceptance and its Impact on Employer Attractiveness,” J. Comput. Inf. Syst., vol. 56, no. 1, pp. 1–10, 2015.

[60] L. Lap, M. Mahinderjit, and A. Samsudin, “Trusted Security Policies for Tackling Advanced Persistent Threat via Spear Phishing in BYOD Environment,” Procedia - Procedia Comput. Sci., vol. 72, pp. 129–136, 2016.

[61] K. Downer and A. D. Challenge, “BYOD Security: A New Business Challenge,” in 2015 IEEE International Conference on Smart City/SocialCom/SustainCom together with DataCom 2015 and SC2 2015 BYOD, 2015, pp. 1128–1133.

[62] A. B. Garba, J. Armarego, and D. Murray, “BRING YOUR OWN DEVICE ORGANISATIONAL INFORMATION SECURITY AND PRIVACY,” vol. 10, no. 3, pp. 1279–1287, 2015.

[63] J. M. King, “Identifying Best Practices for a Byod Policy,” vol. 1277, no. December, p. 48, 2015.

[64] A. Scarfo et al., “Privacy policies for computer forensics,” Comput. Fraud Secur., vol. 4, no. 2, pp. 9–13, 2015.

[65] S. G. Ocano, B. Ramamurthy, and Y. Wang, “Remote mobile screen (RMS): An approach for secure BYOD environments,” in 2015 International Conference on Computing, Networking and Communications, ICNC 2015, 2015.

[66] 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,” ECIS 2015 Res. Pap., pp. 1–10, 2015.

[67] A. Armando, F. B. Kessler, G. Costa, and L. Verderame, “Enabling BYOD through Secure Meta-Market Categories and Subject Descriptors,” in WiSec ’14 Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks, 2014.

[68] P. Bruder, “GADGETS GO TO SCHOOL: The Benefits and Risks of BYOD (Bring Your Own Device),” Educ. Dig., vol. 80, no. 3, pp. 15–18, 2014.

[69] M. Eslahi, M. V. Naseri, H. Hashim, N. M. Tahir, E. Hisham, and M. Saad, “BYOD : Current State and Security Challenges,” pp. 189–192, 2014.

[70] K. Johnson, “An IT CEO talks about the BYOD trend,” Biomed. Instrum. Technol., vol. 48, no. HORIZONS SPRING, pp. 54–56, 2014.

[71] K. Madzima, M. Moyo, and H. Abdullah, “Is bring your own device an institutional information security risk for small-scale business organisations?,” in 2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference, 2014.
S. Marshall, “IT Consumerization: A Case Study of BYOD in a Healthcare Setting,” *Technol. Innov. Manag. Rev.*, vol. 4, no. 3, pp. 14–18, 2014.

Z. Mitrovic, I. Veljkovic, and K. Thompson, “Introducing BYOD in an organisation : the risk and customer services viewpoints,” no. November, 2014.

J. E. Moyer, “Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage,” *J. Hosp. Librariansh.*, no. October 2014, pp. 37–41, 2014.

D. Peraković, S. Husnjak, and I. Cvitić, “Comparative Analysis of Enterprise Mobility Management Systems in BYOD Environment,” *2nd Int. Virtual Res.*, pp. 76–81, 2014.

G. Costantino, F. Martinelli, A. Saracino, and D. Sgandurra, “Towards Enforcing On-The-Fly Policies in BYOD Environments 20J 39th International Conference on Information Assurance and Security (IAS),” in *2013 9th International Conference on Information Assurance and Security (IAS)*, 2013, pp. 61–65.

G. Disteter and C. Kleiner, “BYOD Bring Your Own Device,” *Procedia Technol.*, vol. 9, pp. 43–53, 2013.

B. Dean and E. August, “What is BYOD and why is it important ?,” 2013.

V. Gupta, D. Sangroha, and L. Dhimam, “An Approach to Implement Bring Your Own Device (BYOD) Securely,” *Int. J. Eng. Innov. Res.*, vol. 2, no. 2, pp. 154–156, 2013.

M. Hensema, “Acceptance of BYOD among Employees at Small to Medium-sized Organizations,” *19th Twente Student Conf. IT*, pp. 1–8, 2013.

D. Jaramillo, B. Bodin, S. Cooper, C. H. Becker, and C. Lu, “Mobile innovation applications for the BYOD enterprise user,” vol. 57, no. 6, pp. 1–10, 2013.

B. Longo, “Learning on the Wires: BYOD, Embedded Systems, Wireless Technologies and Cybercrime.,” *Leg. Inf. Manag.*, vol. 13, no. 2, p. 119, 2013.

A. Alharthi, M. O. Alassafi, A. I. Alzahrani, R. J. Walters, and G. B. Wills, “Critical Success Factors for Cloud Migration in Higher Education Institutions: A Conceptual Framework,” *Int. J. Intell. Comput. Res.*, vol. 8, no. 1, pp. 817–825, 2017.

B. B. G. Cesaratto and A. S. Forman, “Cyber Threats to Employee Data and Other Confidential Information Are Front and Center in 2017,” 2017.

J. L. Corchuelo and S. J. Rueda, “AndroidBLP for Confidentiality Management in Android Environments,” *IEEE Lat. Am. Trans.*, vol. 15, no. 3, pp. 496–502, Mar. 2017.

A. Shahrabi, M. Shamizanjani, M. H. Alavidooost, and B. Akhgar, “An Aggregated Fuzzy Model for the Selection of a Managed Security Service Provider,” *Int. J. Inf. Technol. Decis. Mak.*, vol. 16, no. 03, pp. 625–684, 2017.

R. Aserkar, A. Seetharaman, J. A. M. Chu, V. Jadhav, and S. Inamdar, “Impact of personal data protection (PDP) regulations on operations workflow,” *Hum. Syst. Manag.*, vol. 36, no. 1, pp. 41–56, 2017.

M. K. Chihande and J. A. Van Der Poll, “Post cloud computing implementation benefits and challenges realised for a South African technology company,” *2017 Conf. Inf. Commun. Technol. Soc. ICTAS 2017 - Proc.*, 2017.

J. Luckose, S. Chindarkar, and D. Jagli, “Cloud Service Security using Two-factor or Multi
factor Authentication,” Int. Res. J. Eng. Technol., vol. 4, no. 6, pp. 2066–2070, 2017.

[96] A. Musarurwa, S. Flowerday, and L. Cilliers, “Individual traits that determine the Bring Your Own Device information security culture: A case study of the banking sector Individual traits that determine the Bring Your Own Device information security culture: A case study of the banking sector in,” in Information Institute Conferences, Las Vegas, NV, April 18-20, 2017, 2017, no. April.

[97] P. K. Cooper, “ORGANIZATIONAL SECURITY THREATS RELATED TO PORTABLE DATA STORAGE DEVICES: QUALITATIVE EXPLORATORY INQUIRY,” 2017.

[98] C. Banerjee, “Software Security in Requirements Engineering Phase: MCOQR Metrics Framework Perspective,” Int. J. Mod. Comput. Sci., vol. 5, no. 1, pp. 68–74, 2017.

[99] S. Ali, M. N. Qureshi, and A. G. Abbasi, “Analysis of BYOD security frameworks,” Proc. - 2015 Conf. Inf. Assur. Cyber Secur. CIACS 2015, pp. 56–61, 2016.

[100] C. D. Santee, “An Exploratory Study of the Approach to Bring Your Own Device (BYOD) in Assuring Information Security,” no. 1005, 2017.

[101] T. Ulz, T. Pieber, C. Steger, S. Haas, H. Bock, and R. Matischek, “Bring your own key for the industrial Internet of Things,” Proc. IEEE Int. Conf. Ind. Technol., pp. 1430–1435, 2017.

[102] B. J. SHARUM; M. R. Lind, and S. M. Rahman, “Digital natives: The millennial workforce’s intention to adopt bring your own device,” 2017.

[103] S. Tayeb, S. Latifi, and Y. Kim, “A survey on IoT communication and computation frameworks: An industrial perspective,” 2017 IEEE 7th Annu. Comput. Commun. Work. Conf. CCWC 2017, vol. 1301726, pp. 1–6, 2017.

[104] S. N. Grösser, A. Reyes-Lecuona, and G. Granholm, Dynamics of long-life assets: From technology adaptation to upgrading the business model. 2017.

[105] M. Brodin, “Mobile Device Strategy : From a Management Point of View,” J. Mob. Technol. Knowl. Soc., vol. 2017, no. Salesforce 2014, pp. 1–9, 2017.

[106] M. Andrew, F. Barrow, F. Barrow, F. Barrow, and C. Williams, “Folk Risk Analysis : Factors Influencing Security Analysts ’ Interpretation of Risk,” SOUPS (2017)., 2017.

[107] G. Tamman, “Prevention of Service Denial in Collaborative Network,” vol. 4, no. 3, pp. 1–5, 2017.

[108] G. Skinner, “Cyber Security for Younger Demographics A Graphic Based Authentication and Authorisation Framework,” pp. 2487–2490, 2016.

[109] U. Raj and M. S. Catherine, “Certificate based hybrid authentication for Bring Your Own Device (BYOD) in Wi-Fi enabled Environment,” Int. J. Comput. Sci. Inf. Secur., vol. 13, no. 12, pp. 41–47, 2015.

[110] P. Beckett, “BYOD - Popular and problematic,” Netw. Secur., vol. 2014, no. 9, pp. 7–9, 2014.

[111] D. Van Leeuwen, “Bring your own software,” Netw. Secur., vol. 2014, no. 3, 2014.

[112] A. Sedigh, C. Campbell, and K. Radhakrishnan, “BYOT network solutions for enterprise environment,” Proc. - UKSim-AMSS 16th Int. Conf. Comput. Model. Simulation, UKSim 2014, pp. 489–493, 2014.

[113] G. Eschelbeck and D. Schwartzberg, “BYOD risks and rewards,” How to keep Empl. smartphoness. pp. 1–7, 2012.

[114] L. Peterson and C. Scharber, “Lessons From a One-to-One Laptop Pilot,” Comput. Sch., vol. 34, no. 1–2, pp. 60–72, 2017.

[115] M. I. Lali, R. U. Mustafa, F. Ahsan, M. S. Nawaz, and W. Aslam, “Performance Evaluation of Software Defined Networking vs. Traditional Networks,” A quartely Int. Sci. J., vol. 54, no. 1, pp. 16–22, 2017.

[116] C. Paper et al., “Bring-Your-Own-Device ( Byod): Issues and Implementation in Local Colleges and Universities in the ...,” no. October 2013, 2017.

[117] B. Kitchenham, “Procedures for performing systematic reviews,” Br. J. Manag., vol. 14, no. 0, pp. 207–222, 2004.

[118] N. A. A. Bakar, S. Harihodin, and N. Kama, “A Systematic Review of Enterprise Architecture
[119] S. Subramaniam, J. S. Dhillon, M. S. Ahmad, C. Teoh, and W. S. Leong Joyce, “Integrating health behavioural change theories in the design of prediabetes self-care applications: A systematic literature review,” J. Theor. Appl. Inf. Technol., vol. 88, no. 2, pp. 189–201, 2016.

[120] N. Husin, M. T. Abdullah, and R. Mahmood, “A Systematic Literature Review for Topic Detection in Chat Conversation for Cyber-crime Investigation,” Int. J. Digit. Content Technol. Its Appl., vol. 8, no. 18, pp. 22–31, 2014.

[121] T. Kim and H. Kim, “A System for Detection of Abnormal Behavior in BYOD based on Web Usage Patterns,” IEEE, pp. 1288–1293, 2015.

[122] D. Jaramillo, R. Newhook, and R. Smart, “Cross-platform, secure message delivery for mobile devices,” Conf. Proc. - IEEE SOUTHEASTCON, 2013.

[123] W. Pomak and Y. Limpiyakorn, “Enterprise WiFi Hotspot Authentication with Hybrid Encryption on NFC-Enabled Smartphones Wiphop,” IEEE, pp. 247–250, 2018.

[124] Y. Zheng, Y. Cao, and C. H. Chang, “Facial biohashing based user-device physical unclonable function for bring your own device security,” 2018 IEEE Int. Conf. Consum. Electron. ICCE 2018, vol. 2018-January, pp. 1–6, 2018.

[125] C. Kowalevicz, J. Pirrone, and M. Huerta, “Implementation model using a hippocratic protocol in mobile terminals with NFC technology,” 2017 Int. Caribb. Conf. Devices, Circuits Syst. ICCDCS 2017, pp. 113–116, 2017.

[126] Y. C. Kao, Y. C. Chang, and R. S. Chang, “Managing bring your own device services in campus wireless networks,” ICSEC 2015 - 19th Int. Comput. Sci. Eng. Conf. Hybrid Cloud Comput. A New Approach Big Data Era, 2016.

[127] C. Cai, J. Weng, and J. N. Liu, “Mobile authentication system based on national regulation and NFC technology,” Proc. - 2016 IEEE 1st Int. Conf. Data Sci. Cyberspace, DSC 2016, pp. 590–595, 2017.

[128] F. Jaha and A. Kartit, “Pseudo Code of Two-factor Authentication for BYOD,” in 3rd International Conference on Electrical and Information Technologies ICEIT'2017, 2017.

[129] J. Lee, S. Park, and H. Yoon, “Security Policy based Device Management for Supporting Various Mobile OS,” pp. 156–161, 2015.

[130] G. Costantino, F. Martinelli, A. Saracino, and D. Sgandurra, “Towards enforcing on-the-fly policies in BYOD environments,” in 2013 9th International Conference on Information Assurance and Security, IAS 2013, 2014, pp. 61–65.

[131] P. De Las Cuevas, A. M. Mora, J. J. Merelo, P. A. Castillo, P. García-Sánchez, and A. Fernández-Ares, “Corporate security solutions for BYOD: A novel user-centric and self-adaptive system,” Comput. Commun., vol. 68, 2015.

[132] K. Almarhabi, K. Jambi, F. Eassa, and O. Batarfi, “A Proposed Framework for Access Control in the Cloud and BYOD Environment,” IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 2, pp. 144–152, 2018.

[133] N. Kumar Thangaivelan, E. Niguissie, A. Hakkala, S. Virtanen, and J. Isoaho, “CoDRA: Context-based dynamically reconfigurable access control system for android,” J. Netw. Comput. Appl., vol. 101, pp. 1–17, 2018.

[134] I. Musulukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, “Understanding users’ requirements for data protection in smartphones,” Proc. - 2012 IEEE 28th Int. Conf. Data Eng. Work. ICDEW 2012, pp. 228–235, 2012.

[135] A. Roy and D. Dasgupta, “A fuzzy decision support system for multifactor authentication,” Soft Comput., vol. 22, no. 12, pp. 3959–3981, 2018.

[136] N. Agrawal and S. Tapaswi, “Access Control Framework Using Dynamic Attributes Encryption for Mobile Cloud Environment,” in Advances in Intelligent Systems and Computing, Springer Nature Singapore Pte Ltd., 2018, pp. 611–621.

[137] F. Jaha and A. Kartit, Improving Implementation of Keytroke Dynamics Using K-NN and Manhattan Distance, vol. 872, no. 1. Springer International Publishing, 2018.
[138] A. G. Kravets, N. D. Bui, and M. Al-Ashval, “Mobile Security Solution for Enterprise Network,” Commun. Comput. Inf. Sci., vol. 466 CCIS, pp. 371–382, 2014.

[139] A. Wójtowicz and K. Joachimiak, “Model for adaptable context-based biometric authentication for mobile devices,” Pers. Ubiquitous Comput., vol. 20, no. 2, pp. 195–207, 2016.

[140] T. Galibus et al., “Offline Mode for Corporate Mobile Client Security Architecture,” Mob. Networks Appl., vol. 22, no. 4, pp. 743–759, 2017.

[141] S. W. Park, J. N. Kim, and D. G. Lee, “SecureDom: secure mobile-sensitive information protection with domain separation,” J. Supercomput., vol. 72, no. 7, pp. 2682–2702, 2016.

[142] F. Jamal, M. T. Abdullah, A. Abdullah, and Z. M. Hanapi, “Enhanced Bring your Own Device (BYOD) Environment Security based on Blockchain Technology,” Int. J. Eng. Technol., vol. 7, pp. 74–79, 2018.