ISSN : 1411-1624
e-ISSN: 2621-8089

PEMILIHAN SOLUSI PENERAPAN *BRING YOUR OWN DEVICE* (BYOD) BERDASARKAN KONTROL KEAMANANNYA

Moh. Idris
Dosen Universitas Islam Indonesia
Jalan Kaliurang km. 14,5 Sleman Yogyakarta
Sur-el : moh.idris@uii.ac.id

Abstract : *The term BYOD (Bring Your Own Device) refers to the use of employees' personal devices (for example smartphones, tablets, laptops, netbooks) to do their work and manage corporate data from anywhere at any time. BYOD has been widely applied in the business world, hospitals, and education. With the ease that can be achieved by using BYOD, the security aspect is very important to consider. It starts with the security of the device to the security of company data that can be accessed by employees. Five dimensions of security control that must be considered in implementing BYOD: 1) data control; 2) access control; 3) network access control; 4) device management; 5) create a supporting framework. With the five BYOD implementation solutions presented in this study, there is only one solution that accommodates the five dimensions of BYOD security control, the use of Mobile Device Management (MDM) technology.*

Keywords: *BYOD, security control, access control, network access control, virtualization, cloud computing*

Abstrak : *Istilah BYOD (Bring Your Own Device) mengacu pada penggunaan perangkat pribadi karyawan (misalnya ponsel cerdas, tablet, laptop, netbook) untuk melakukan pekerjaan mereka dan mengelola data perusahaan dari mana saja kapan saja. BYOD telah banyak diterapkan di dunia bisnis, rumah sakit, dan pendidikan. Dengan kemudahan yang dapat dicapai dengan menggunakan BYOD, aspek keamanan sangat penting untuk dipertimbangkan. Dimulai dengan keamanan perangkat hingga keamanan data perusahaan yang dapat diakses oleh karyawan. Lima dimensi kontrol keamanan yang harus dipertimbangkan dalam mengimplementasikan BYOD: 1) kontrol data; 2) kontrol akses; 3) kontrol akses jaringan; 4) manajemen perangkat; 5) membuat kerangka kerja pendukung. Dengan lima solusi implementasi BYOD yang disajikan dalam penelitian ini, hanya ada satu solusi yang mengakomodasi lima dimensi kontrol keamanan BYOD yaitu pengunaan teknologi Mobile Device Management (MDM).*

Kata kunci*: BYOD, kontrol keamanan, kontrol akses, kontrol jaringan, virtualisasi, cloud computing*

1. PENDAHULUAN

Penetrasi Internet dalam kehidupan sehari-hari menjadi salah satu faktor munculnya praktik konsumerisasi di bidang teknologi informasi (TI) akhir-akhir ini. Konsumerisasi merujuk pada penggunaan perangkat pribadi oleh pengguna ke dalam sektor bisnis dan pendidikan [1] karena pengguna sudah merasa familiar dengan perangkat pribadi mereka dalam kehidupan sehari-hari [2,3]. Salah satu pendorongnya adalah berkembangnya teknologi perangkat bergerak (*mobile device*), seperti smartphone dan tablet, yang mempunyai ukuran lebih kecil dan ringan dengan konsumsi daya yang rendah sehingga menjadi lebih populer [4] ketika dari dari segi kecepatan dan kapasitas penyimpanannya sudah hampir menyamai komputer. Dengan adanya konsumerisasi TI maka terjadi perubahan yang mendasar tentang

ISSN : 1411-1624
e-ISSN: 2621-8089

bagaimana seseorang menyelesaikan pekerjaannya dengan menggunakan perangkat yang ia miliki sehingga pasar konsumen sekarang sudah menjadi pendorong utama terkait dengan inovasi di bidang TI.

Salah satu efek yang ditimbulkan oleh konsumerisasi TI adalah munculnya istilah *Bring Your Own Device* (BYOD) atau Bawa Perangkat Anda Sendiri yang merujuk pada adopsi perangkat pribadi oleh seseorang (berupa *smartphone*, tablet atau laptop) untuk melakukan pekerjaan kantor (seperti penggunaan surel dan basisdata perusahaan serta untuk membuat, menyimpan dan mengatur data perusahaan [5] sekaligus untuk penggunaan pribadi [6,7,8]. Penggunaan BYOD tidak hanya terjadi pada kegiatan di sektor bisnis saja, akan tetapi juga meluas ke sektor-sektor lainnya seperti pendidikan/sekolah [9,10] dan sektor kesehatan/rumah sakit [11]. Hal ini disebabkan karena ada beberapa keuntungan dengan adanya praktek BYOD di sektor-sektor tersebut, salah satunya adalah terkait produktifitas yang lebih tinggi ketika seseorang tetap dapat bekerja di luar jam kantor melalui perangkat pribadinya dimanapun dan kapanpun ia berada. BYOD dianggap dapat meningkatkan efisiensi dan produktivitas, meningkatkan kepuasan dan mobilitas pekerjaan, dan menawarkan keunggulan kompetitif dibandingkan perusahaan lain [12,13]. Ketika seorang karyawan bekerja dengan perangkat yang mereka pilih sendiri maka mereka akan lebih akrab dengan teknologi yang digunakan [13,3] dan hal ini dapat meningkatkan kepuasan dalam bekerja [13]. Di sisi perusahaan, penerapan BYOD dapat menekan pengeluaran terkait dengan pengadaan perangkat yang digunakan oleh karyawan untuk bekerja [14] dan perusahaan dapat mengalihkan fokus untuk memperbaiki dukungan TI dalam rangka memfasilitasi koneksi yang dapat diandalkan antara perangkat karyawan dengan server perusahaan [13].

Selain memiliki beberapa keuntungan, penerapan BYOD juga memiliki resiko yang harus diperhatikan oleh setiap perusahaan atau organisasi yang ingin menerapkannya. Salah satu contoh resiko yang muncul adalah kerentanan data/informasi. Saat ini, informasi merupakan aset penting bagi sebuah perusahaan dibandingkan dengan aset fisik sehingga sangat penting sekali menjaga informasi-informasi tersebut. Di satu sisi BYOD merupakan salah satu penyebab baru terkait kerentanan data dan informasi yang terjadi ketika karyawan mengakses data sensitif milik perusahaan menggunakan perangkat pribadi mereka yang digunakan untuk bekerja [15]. Perusahaan yang memperbolehkan praktek BYOD di lingkungan kerja mereka harus mempunyai prioritas untuk menjaga prinsip dasar keamanan informasi mulai dari ketersediaan, integritas, dan kerahasiaan.

Beberapa penelitian telah memberikan alternatif-alternatif solusi yang dapat digunakan untuk mengatasi beberapa masalah/resiko yang ditimbulkan dari penggunaan BYOD. Namun, penerapan solusi-solusi yang ada tidak serta merta dapat diterapkan begitu saja karena setiap alternatif solusi mempunyai karakteristik sendiri-sendiri. Agar penerapan solusi yang ada dapat dilakukan secara optimal, maka perlu diketahui terlebih dahulu karakteristik dari masing-masing

ISSN : 1411-1624
e-ISSN: 2621-8089

solusi yang ditawarkan agar sesuai dengan aspek-aspek keamanan yang ingin diterapkan.

2. METODOLOGI PENELITIAN

2.1 Studi Literartur

2.1.1 BYOD

BYOD adalah konsep yang memungkinkan karyawan untuk memanfaatkan teknologi dan perangkat milik pribadi mereka untuk tetap terhubung, mengakses data perusahaan, atau menyelesaikan tugas dari perusahaan [16]. Pada dasarnya BYOD adalah suatu pendekatan yang karyawan suatu perusahaan menggunakan peralatan TIK mereka sendiri untuk melakukan pekerjaan mereka alih-alih menggunakan peralatan yang disediakan oleh perusahaan mereka [17].

Perangkat yang digunakan dalam praktik BYOD dapat berupa laptop, netbook, tablet, smartphone. *Smartphone* sangat umum digunakan dalam BYOD karena mudah dibawa, dapat terhubung ke Internet di mana saja dengan mudah, dan menyediakan berbagai aplikasi [18]. Ketika smartphone dan tablet menjadi populer di tempat kerja, maka istilah BYOD sering digunakan untuk merujuk ke perangkat seluler ini [14].

Penggunaan BYOD tidak hanya terbatas pada perusahaan yang bergerak di sektor bisnis saja. Di dunia pendidikan dan kesehatan juga tidak lepas dari penetrasi penggunaan BYOD. BYOD di bidang pendidikan dapat diartikan dengan penggunaan perangkat pribadi oleh siswa yang bertujuan untuk mendukung belajar [19]. BYOD juga termasuk dalam jenis *mobile learning* [20]. Di bidang kesehatan beberapa pihak rumah sakit sudah memperbolehkan penggunaan perangkat pribadi untuk bekerja [11]. Praktik BYOD muncul sebagai bentuk efisiensi anggaran jangka pendek yang dilakukan oleh rumah sakit [11].

2.1.2 Keuntungan BYOD

Penerapan BYOD memiliki beberapa keuntungan, yaitu:

a) Efisiensi anggaran, Perusahaan dapat memangkas biaya TI mereka ketika karyawan berinvestasi dalam perangkat kerja mereka masing-masing [21],
b) Peningkatan mobilitas dan produktifitas karyawan, Karena menggunakan perangkat sendiri untuk bekerja, maka karyawan dapat melakukan pekerjaan mereka kapan pun dan dimana pun mereka berada sehingga produktifitas juga ikut meningkat [13],
c) Kenyamanan, Hal ini dapat dicapai karena karyawan bekerja menggunakan perangkat mereka sendiri sehingga mereka sudah terbiasa dengan teknologi perangkat yang digunakan dan merasa nyaman dalam bekerja [1,13],
d) Aksesibilitas, BYOD memungkinkan akses dan pengambilan sumber daya dan materi yang dimiliki perusahaan secara daring. Hal ini dapat memungkinkan karyawan untuk mengakses sumber daya jaringan yang disediakan oleh perusahaan mereka, dan belajar atau bekerja dengan sumber daya ini sesuai keinginan mereka [22].

ISSN : 1411-1624
e-ISSN: 2621-8089

2.1.3 Resiko/Ancaman BYOD

Selain menawarkan beberapa keuntungan, penerapan BYOD juga memiliki beberapa resiko/ancaman yang dapat terjadi setiap saat. Beberapa resiko/ancaman tersebut adalah:

a) Keamanan, Isu keamanan berkaitan dengan transmisi dan penyimpanan data perusahaan yang terjadi di perangkat pribadi karyawan [23],
b) Ketika data perusahaan dapat diakses oleh perangkat pribadi karyawan, maka keamanan perangkat tersebut harus ditingkatkan,
c) Kurangnya kontrol terhadap perangkat, Kurangnya kontrol terhadap perangkat yang digunakan oleh masing-masing karyawan menjadi salah satu resiko dari penerapan BYOD [6]. Misalnya kerusakan perangkat serta aplikasi-aplikasi yang dipasang di dalam perangkat pengguna tidak dapat dikontrol oleh pihak perusahaan [24],
d) Data perusahaan semakin rentan
   Kehilangan perangkat yang digunakan oleh karyawan dapat menyebabkan kehilangan data perusahaan yang terdapat di dalam perangkat tersebut sehingga dapat diakses oleh orang lain [24]. Selain itu, infrastuktur dan data yang dimiliki oleh perusahaan mengalamin perubahahan yang semula berada di lingkungan yang tertutup menjadi berada di lingkungan yang terbuka sehingga akses dari perangkat pribadi diperbolehkan setiap saat dan dari manapun.
e) Privasi Ketika perangkat seluler dirancang untuk mengakses BYOD digunakan untuk keperluan pribadi dan bisnis maka data pribadi pengguna akhir seperti kontak, alamat, foto dan dokumen harus dilindungi dari akses oleh pihak perusahaan [1].
f) Ancaman *cybercrime*
   Sikap dan perilaku karyawan juga dapat berkontribusi dalam munculnya ancaman seperti malware dan virus, dan kerentanan lainnya [25]. *Malware* dan virus dapat masuk ke dalam perangkat melalui aplikasi pihak ketiga yang didapat dari sumber yang tidak terpercaya. Penggunaan jaringan nirkabel yang tidak aman, misalnya di tempat umum, dapat juga menjadi pintu masuk *malware* ke dalam perangkat yang digunakan. Ketika *malware* sudah masuk ke dalam perangkat, maka hal itu dapat membahayakan data perusahaan yang tersimpan di dalamnya atau bahkan dapat menjadi pintu masuk untuk masuk ke dalam sistem perusahaan ketika perangkat tersebut terhubung dengan jaringan perusahaan.

2.1.4 Solusi Penerapan BYOD

a. Virtualisasi dekstop/aplikasi

Pendekatannya didasarkan pada konsep bahwa aktor utama di dalam ruang kerja adalah para pengguna/karyawan dan semua yang ada di sekitar mereka harus dibuat senyaman mungkin. Sumber daya TI dibuat menggunakan teknik virtualisasi sehingga aspek keamanan, *firewall*, *backup*, enkripsi data, hingga keberlangsungan bisnis diatur oleh perusahaan secara terpusat [6]. Pendekatan ini menempatkan pengguna sebagai pusat penerapan BYOD.

b. Kontrol perangkat

Pendekatannya didasarkan pada konsep yang mendukung kontrol penuh terhadap perangkat yang digunakan mulai dari enkripsi, aplikasi-aplikasi yang

ISSN : 1411-1624
e-ISSN: 2621-8089

boleh dipasang, mengunci perangkat, hingga menerapkan aturan-aturan perusahan terhadap perangkat yang digunakan oleh para karyawan [6]. Pendekatan ini menempatkan perangkat sebagai pusat penerapan BYOD.

c. Kontrol akses jaringan

Pendekatan ini memungkinkan perusahaan untuk mengidentifikasi setiap perangkat yang digunakan oleh pengguna dan mengaplikasikan aturan keamanan sebelum memperbolehkan akses terhadap sumberdaya yang dimiliki oleh perusahaan [23].

d. *Virtual Private Network* (VPN)

Implementasi VPN atau jenis komunikasi terenkripsi lainnya dalam BYOD akan menyediakan akses terbatas ke jaringan perusahaan untuk komunikasi antara perangkat dan server. Adopsi VPN sebagai kontrol keamanan untuk praktik BYOD akan memicu perangkat lunak klien VPN diinstal dan dikonfigurasikan dengan benar pada perangkat pengguna. Praktik ini akan meringankan kesalahan pengguna dan perusahaan ketika terjadi insiden keamanan yang melibatkan perangkat pengguna dan akan semakin memperkuat adopsi VPN sebagai cara untuk mengamankan praktik BYOD [26].

e. Cloud Computing Management

Penggunaan *cloud computing* untuk penerapan BYOD menyediakan tingkat keamanan seperti lingkungan yang terisolasi dan servis yang sangat terkontrol sehingga tingkat perlindungan yang diperlukan dan layak untuk aset tertentu harus diprioritaskan.

2.1.5 Dimensi Keamanan BYOD

Terdapat lima dimensi yang berhubungan dengan kontrol keamanan pada penerapan BYOD yaitu [23]:

a. Kontrol Data: adalah proses yang dilakukan dengan mengontrol sumber data dengan cara membatasi apa saja yang dapat diunduh oleh pengguna melalui perangkat mereka.
b. Kontrol Akses: adalah proses meningkatkan metode kontrol akses yang sudah ada dengan mempertimbangkan faktor-faktor kontekstual yang ada seperti level resiko yang dihadapi serta level kepercayaan pengguna perangkat terhadap akses perusahaan kepada perangkat mereka.
c. Kontrol Jaringan: adalah proses mengorganisasi jaringan yang digunakan oleh perusahaan dengan cara mengontrol dan mengawasi perangkat pihak ketiga yang terkoneksi dengan jaringan tersebut.
d. Manajemen Perangkat: adalah proses untuk mengatur perangkat yang digunakan dalam praktik BYOD oleh pengguna maupun perusahaan seperti proses autentifikasi yang lebih baik, pengendalian data, serta kemampuan untuk mengatur perangkat secara jarak jauh.
e. Pembuatan Kerangka Kerja Pendukung: berupa kebutuhan kontrol non-teknis seperti peraturan-peraturan, pelatihan, serta peningkatan kesadaran pengguna.

2.2 Metode Penelitian

2.2.1 Pengumpulan Data

Artikel-artikel yang digunakan dalam penelitian ini bersumber dari sejumlah jurnal yang didapat melalui pencarian lewat *Google Scholar*. Kata kunci yang digunakan pada

ISSN : 1411-1624
e-ISSN: 2621-8089

proses pencarian adalah *Bring Your Own Device* dan BYOD.

2.2.2 Penyaringan Artikel

Setelah artikel terkumpul maka langkah selanjutnya adalah menyaring artikel-artikel tersebut. Artikel yang akan dijadikan bahan kajian adalah yang terbit antara tahun 2012 hingga tahun 2017, judul artikel, abstraksi, dan kata kunci yang ada di dalam artikel tersebut. Fokus penyaringan dilakukan berdasarkan kata kunci resiko, kontrol, keamanan, ancaman, manfaat, dan solusi penerapan BYOD.

2.2.3 Analisis Temuan

Pada langkah ini, data-data yang sudah terkumpul dan sudah tersaring akan dianalisis untuk mendapatkan beberapa solusi untuk menerapkan praktik BYOD. Setelah itu solusi-solusi yang didapatkan akan dipetakan berkaitan dengan lima dimensi kontrol keamanan pada penerapan BYOD untuk melihat kontrol keamanan mana saja yang terdapat pada solusi-solusi tersebut.

3. HASIL DAN PEMBAHASAN

Pada bagian ini akan dilakukan pemetaan dari beberapa solusi penerapan BYOD yang sudah dipaparkan sebelumnya berdasarkan lima dimensi kontrol keamanan BYOD berupa kontrol data, kontrol akses, kontrol jaringan, manajemen perangkat dan pembuatan kerangka kerja pendukung. Untuk hasil pemetaan dapat dilihat pada Tabel 1.

Berdasarkan data yang terdapat pada Tabel 1 hanya ada satu solusi yang mencakup kelima dimensi kontrol keamanan BYOD. Berikut ini adalah pembahasan lebih detilnya.

Beberapa alasan utama yang menjadikan penggunaan teknik virtualisasi menjadi cara yang efisien untuk imlementasi BYOD adalah sebagai berikut [6]:

a. Penggunaan virtualisasi dan data terpusat menjadikan perusahaan dapat mengimplementasikan keamanan yang lebih baik termasuk enkripsi data, sistem pendeteksi gangguan dan backup.
b. Virtualisasi juga menerapkan kontrol seperti penolakan proses salin dan tempel data antara mesin virtual dan perangkat yang digunakan serta pembatasan kemampuan untuk mencetak konten/dokumen.
c. Perusahaan dapat melindungi data karena konten dari sistem virtualisasi tidak disimpan di perangkat sehingga dapat memastikan keamanan data apabila perangkat yang digunakan hilang atau dicuri.

Tabel 1. Pemetaan Solusi Penggunaan BYOD

Solusi Penerapan BYOD	***Dimensi Kontrol Keamanan BYOD***				
	Kontrol Data	***Kontrol Akses***	***Kontrol Jaringan***	***Manajemen Perangkat***	***Pembuatan Kerangka Kerja Pendukung***
Virtualisasi dekstop/aplikasi	√	√	-	-	√
Kontrol perangkat	√	√	√	√	√
Kontrol akses jaringan	-	√	√	-	√
Virtual Private Network (VPN)	-	√	√	-	√
Cloud Computing Management	√	√	√	-	√

ISSN : 1411-1624
e-ISSN: 2621-8089

Solusi berupa kontrol perangkat memudahkan perusahaan/instansi/organisasi untuk mengontrol perangkat yang digunakan. Dengan menggunakan API tertentu perangkat bergerak yang digunakan dalam BYOD dapat dikontrol [6]. Salah satu model penerapannya adalah teknologi *Mobile Device Management* (MDM). Perangkat lunak MDM menyediakan cara untuk membuat daftar hak tentang siapa yang memiliki perangkat apa dan otoritas seperti apa untuk mengakses aplikasi internal perusahaan [27]. Pendekatan MDM didasarkan pada kontrol ketat dari perangkat yang memungkinkan perusahaan untuk mengontrol, mengelola dan memantau data, aplikasi, pengaturan perangkat, penggunaan jaringan, bersama dengan pemanfaatan perangkat dan perilaku pengguna [6].

Solusi kontrol akses jaringan bertujuan untuk otentikasi pengguna dan kontrol akses [27]. Solusi mengontrol akses jaringan pengguna dengan mengidentifikasi pengguna yang diautentikasi atau memaksa kepatuhan dengan kebijakan keamanan. Pengaturan akses jaringan ini sangat penting karena perangkat seluler yang dapat terhubung dari jarak jauh ke jaringan perusahaan dari mana saja dan kapan saja dapat membuat jaringan dan data perusahaan berisiko. Solusi ini diperkenalkan dengan tujuan untuk memblokir akses jaringan oleh PC yang terinfeksi untuk mencegah penyebaran kode jahat di jaringan internal perusahaan [27].

Penggunaan VPN dapat menyediakan fasilitas kerahasiaan data, integritas data, dan integritas antara perangkat pengguna dan jaringan milik perusahaan serta server yang digunakan. Perangkat pengguna pertama kali akan diotentikasi selama fase awal komunikasi melalui VPN, diikuti dengan sesi aman melalui enkripsi dan kode otentikasi pesan untuk komunikasi berikutnya dan pertukaran data antara perangkat pengguna dan sistem perusahaan [26].

Pada penerapan *cloud computing* pada BYOD, ada tiga zona keamanan yang diterapkan dalam model ini yaitu: kontrol keamanan untuk pengguna dan semua perangkat, keamanan jaringan yang digunakan oleh perangkat, serta keamanan *cloud* yang disediakan oleh vendor [28]. Strategi yang dapat digunakan untuk mengamankan zona tersebut dari sisi perusahaan antara lain [23]:

a. Mengamankan akses ke *cloud* dengan menggunakan teknik manajemen identitas, termasuk otentikasi yang kuat. Hal ini sangat disarankan menggunakan otentikasi multifaktor.
b. Mendistribusikan aset sebagai potongan-potongan di antara banyak *cloud*. Hal ini bertujuan jika salah satu cloud dapat dicuri maka sumber daya yang ada *cloud* tersebut tidak akan memiliki nilai tanpa digabung dengan sumber daya lain yang disimpan di *cloud* lainnya.
c. Menentukan kelas layanan keamanan *cloud* berdasarkan pada profil keamanan dan kepercayaan untuk para penyedia layanan *cloud*. Klasifikasi ini akan membantu menentukan pembagian aset yang akan diletakkan di beberapa penyedia *cloud* yang berbeda dengan mempertimbangkan tingkat keamanan yang sesuai untuk masing-masing aset.

ISSN : 1411-1624
e-ISSN: 2621-8089

4. KESIMPULAN

Berdasarkan proses dan hasil penelitian yang telah dilakukan, maka dapat ditarik beberapa kesimpulan sebagai berikut:

a. Dari beberapa solusi penerapan BYOD dalam penelitian ini hanya ada satu solusi saja yang mencakup semua aspek dimensi kontrol keamaan BYOD yaitu kontrol perangkat dengan menggunakan teknologi MDM.
b. Faktor seperti pemilihan dimensi kontrol mana saja yang akan diterapkan akan mempengaruhi solusi yang akan diambil oleh perusahaan dan hal tersebut juga tergantung pada budaya organisasi dan anggaran keamanan TI yang sudah dipatok oleh masing-masing perusahaan.
c. Kebutuhan kontrol non-teknis seperti peraturan-peraturan yang diterapkan di sebuah perusahaan perlu ditinjau ulang setiap saat agar penerapannya sesuai dengan tren BYOD yang sedang berlangsung saat itu.
d. Pelatihan terkait dengan solusi BYOD yang sudah atau akan diterapkan juga perlu dilakukan secara berkala agar praktik yang dilakukan oleh pengguna sesuai dengan yang diinginkan oleh perusahaan.
e. Kesadaran pengguna terutama terkait dengan aspek keamanan perangkat mereka masing-masing juga perlu ditingkatkan agar mampu mendukung praktik BYOD oleh perusahaan.
f. Pembahasan dimensi keamanan BYOD pada bagian pembuatan kerangka kerja pendukung belum dapat dieksplorasi lebih dalam di dalam pembahasan karena bagian tersebut dianggap akan dilakukan oleh masing-masing perusahaan ketika akan menerapkan sebuah solusi BYOD. Hal ini perlu diteliti lagi pada penelitian berikutnya.

DAFTAR PUSTAKA

[1] G. Disterer and C. Kleiner, “BYOD bring your own device,” *Procedia Technology*, vol. 9, pp. 43-53, 2013.
[2] A. György, A. Cleven, F. Uebernickel, and W. Brenner, “Exploring the shadows: IT governance approaches to user-driven innovation,” *ECIS 2012 Proceedings*, pp. 222, 2012.
[3] M. Harris, K. Patten, E. Regan and J. Fjermesat, “Mobile and Connected Device Security Considerations: A Dilemma for Small and Medium Enterprise Business Mobility?,” *Proc. of the 18th Americas Conference on Information Systems (AMCIS)*, pp. 1-7, 2012.
[4] G. Kulkarni, R. Shelke, R. Palwe, V. Solanke, S. Belsare, and S. Mohite, “Mobile cloud computing-bring your own device,” in *2014 Fourth International Conference on Communication Systems and Network Technologies*, pp. 565-568, 2014.
[5] Osterman-Research, "Living With BYOD in Your Organization," 2014.
[6] A. Scarfo, “New security perspectives around BYOD,” in *2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications*, pp. 446-451, 2012.
[7] 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,” 2013.
[8] U. Vignesh and S. Asha, Modifying security policies towards BYOD,” *Procedia Computer Science*, vol. 50, pp. 511-516, 2015.
[9] Y. Song, and S. C. Kong, “Affordances and constraints of BYOD (Bring Your Own Device) for learning and teaching in higher education: Teachers’ perspectives,” *The Internet and Higher Education*, vol. 32 no. 1, pp. 39-46, 2017.
[10] P. N. Chou, C. C. Chang and C. H. Lin, “BYOD or not: A comparison of two assessment strategies for student learning,”

ISSN : 1411-1624
e-ISSN: 2621-8089

Computers in Human Behavior, vol. 74, pp. 63-71, 2017.

[11] J. E. Moyer, "Managing mobile devices in hospitals: A literature review of BYOD policies and usage," *Journal of Hospital Librarianship*, vol. 13 no. 3, pp. 197-208, 2013.

[12] N. Singh, "BYOD genie is out of the bottle–"Devil or angel"," *Journal of Business Management & Social Sciences Research*, vol. 1 no. 3, pp. 1-12, 2012.

[13] T. Shumate, and M. Ketel, "Bring your own device: benefits, risks and control techniques," in *IEEE Southeastcon 2014*, pp. 1-6, 2014.

[14] Y. Wang, J. Wei and K. Vangury, "Bring your own device security issues and challenges," in *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*, pp. 80-85, 2014.

[15] D. Peraković, S. Husnjak, V. Mišićand T. Kuljanić, "Employee's awareness on security aspects of use bring your own device paradigm in Republic of Croatia," in *The 4th International Virtual Research Conference In Technical Disciplines (RCITD2016)*, 2016.

[16] R. Afreen, "Bring your own device (BYOD) in higher education: opportunities and challenges," *International Journal of Emerging Trends & Technology in Computer Science*, vol. 3 no. 1, pp. 233-236, 2014.

[17] 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*, pp. 1-8, 2014.

[18] S. Tanimoto, S. Yamada, M. Iwashita, T. Kobayashi, H. Sato A. Kanai, "Risk assessment of BYOD: Bring your own device," in *2016 IEEE 5th Global Conference on Consumer Electronics*, pp. 1-4, 2016.

[19] D. Nelson, "BYOD: An opportunity schools cannot afford to miss," *Internet@ schools*, vol. 19 no. 5, pp. 12-15, 2012.

[20] G. J. Hwang and C. C. Tsai, "Research trends in mobile and ubiquitous learning: A review of publications in selected journals from 2001 to 2010," *British Journal of Educational Technology*, vol. 42 no. 4, pp. E65-E70, 2011.

[21] M. Eslahi, M. V. Naseri, H. Hashim, N. N. Tahir, and E. H. M. Saad, "BYOD: Current state and security challenges," in *2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE)*, pp. 189-192, 2014.

[22] A. B. Garba, J. Armarego, D. Murray and W. Kenworthy, "Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments," *Journal of Information privacy and security*, vol. 11 no. 1, pp. 38-54, 2015

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

[24] K. AlHarthy and W. Shawkat, "Implement network security control solutions in BYOD environment," in *2013 IEEE International Conference on Control System, Computing and Engineering*, pp. 7-11, 2013.

[25] B. Tokuyoshi, "The security implications of BYOD," *Network Security*, vol. 4, pp. 12-13, 2013.

[26] T. A. Yang, R. Vlas, A. Yang and C. Vlas, "Risk management in the era of byod: the quintet of technology adoption, controls, liabilities, user perception, and user behavior," in *2013 International Conference on Social Computing*, pp. 411-416, 2015.

[27] E. B. Koh, J. Oh, and C. Im, "A study on security threats and dynamic access control technology for BYOD, smart-work environment," in *Proceedings of the International MultiConference of Engineers and Computer Scientists*, vol. 2, pp. 1-6, 2014.

[28] E. G. Amoroso, "From the enterprise perimeter to a mobility-enabled secure cloud," *IEEE Security & Privacy*, vol. 11 no. 1, pp. 23-31, 2013.